Electronic Mail

MODULE 16

Contents

16.1 Learning Objectives....4

16.2 Electronic Mail (E-mail) 4

16.2.1 E-mail Message Components....5

16.2.1.1 Header 5

16.2.1.2 Message Body....6

16.2.2 Components of an E-mail System 6

16.2.2.1 User Agent (UA) 6

16.2.2.2 Message Transfer Agent (MTA) 6

16.2.2.3 Message Access Agent (MAA)....7

16.2.2.4 Spool....7

16.2.2.5 Mailbox....7

16.3 Architecture of E-mail....7

16.4 Protocols used in email systems 8

16.4.1 SMTP 8

16.4.2 POP3....9

16.4.3 IMAP....9

16.5 Differences between POP3 and IMAP.... 10

16.6 Working of E-mail.... 10

16.7 Types of E-mail.... 12

16.7.1 Advantages of e-mail.... 13

16.7.2 Disadvantages of Email.... 13

16.8 E-mail Attack.... 14

16.8.1. Spam.... 14

16.8.2 Phishing Attacks.... 15

16.8.3 Spear phishing 15

16.8.4 Whaling Email Attack.... 15

16.8.5 Virus 16

16.8.6 Pharming.... 16

16.8.7 Ransomware.... 17

16.8.8 Spyware 17

16.8.9 Business Email Compromise (BEC) Attacks 17
16.8.10 Account Take Over (ATO) Attack 18
16.9 E-mail Security 18
16.9.1 Organization Email Security Best Practices 18
16.9.2 Individual User Email Security Best Practices 19
16.10 Email attacks and crimes 20
16.10.1 Flaming 20
16.10.2 Email spoofing 20
16.10.3 Email bombing 20
16.10.4 Email hacking 20
16.10.5 Spams 21
16.10.6 Phishing 21
16.10.7 Email fraud 21
16.10.8 Phishing emails 21
16.11 Privacy in emails 21
16.11.1 Email privacy 21
16.11.2 Email tracking 22
10.12 Summary 22
10.13 Check Your Progress 23
10.14 Model Questions 24
10.15 Further Readings 25
References, Article Source & Contributors 25

Electronic Mail

16.1 LEARNING OBJECTIVES

After the completion of this unit the learner shall be able to:

- **Expain emailing and email services.**
- **Corelate the structure of email to extract forensic information.**
- **Categorize email attacks and crimes.**
- **Use few email forensic tools.**

16.2 ELECTRONIC MAIL (E-MAIL)

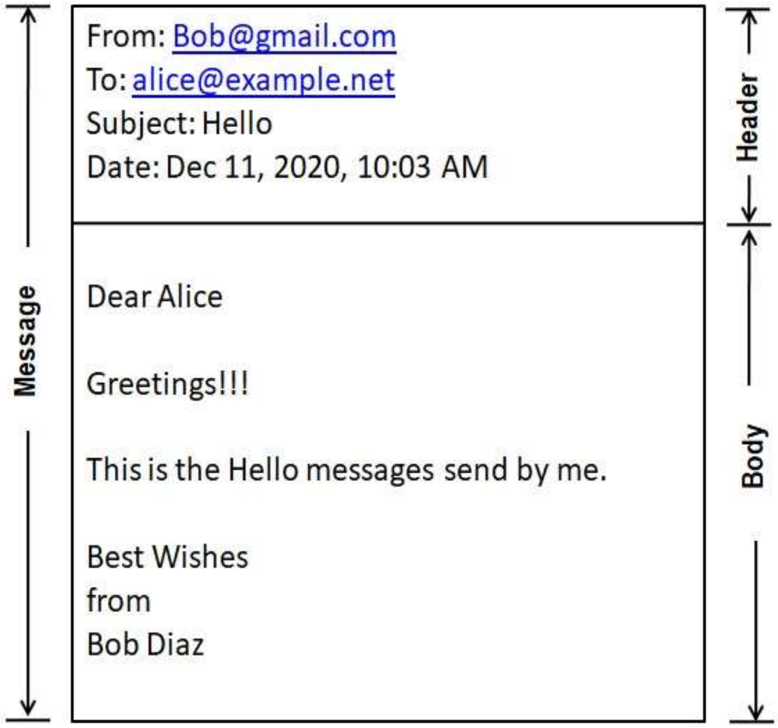
VIDEO LECTURE

E-mail refers to the transmission of messages through the Internet. It is one of the most commonly used technologies on communication networks that may include text, images, audio, video and/or other attachments. In general, the e-mail systems are based on a store-

and-forward **model and can also send a message to one or more recipients. Neither the users and nor their computers are required to be online at the same time; they need to connect, typically to an e-mail server or a** webmail **interface to send or receive messages or download it. E-mail servers are capable of accepting, transferring, delivering and storing messages. The list of some free e-mail service providers are AOL, Gmail, Microsoft Outlook, ProtonMail, Rediffmail, Yahoo Mail, Zoho and so on.**

16.2.1 E-mail Message Components

The e-mail contains delivery information along with content. It complies with certain standards set by The Internet Engineering Task Force (IETF) [https://www.ietf.org/], so that e- mail can be processed by the various computer systems. An email message consists of two main sections: the header and the body, which has been shown in below figure.



From: Bob@gmail.com
To: alice@example.net
Subject: Hello
Date: Dec 11, 2020, 10:03 AM

Dear Alice

Greetings!!!

This is the Hello messages send by me.

Best Wishes
from
Bob Diaz

Figure 1: E-mail Message Components

16.2.1.1 Header

The e-mail header contains multiple lines, each of which start with a keyword followed by a colon and additional information. A typical e-mail header contains the *From*, *To*, *Subject* and *Date.* The From field indicates the e-mail address of the sender. Email addresses are always made up of a username followed by a @ sign and a domain name. For instance, Bob@gmail.com is an email address where ‘Bob' is the username and ‘gmail.com' is a domain name. The To field indicates the e-mail address of the recipient. The Date field shows the date in which the e-mail was sent. The Subject field specifies the topic of the e-mail precisely. Additionally, there are more header lines in most e-mails: Cc and Bcc. The Cc refers to carbon copy. The e-mail address provided on the Cc header must receive an exact copy of the message. Furthermore, all the e-mail message recipients receive the *To* and *cc* header lines. The Bcc signifies Black Carbon Copy. The e-mail address referred in the Bcc header must get a blind carbon copy of the message. Although, The Bcc header line is not delivered to e-mail recipients.

16.2.1.2 Message Body

The body of the message contains the information that the recipients have to read. The information can be written with text in various character sets, Hypertext Markup Language (HTML), attached files with different format or multimedia content, and so forth.

16.2.2 Components of an E-mail System

The basic components of an e-mail system are: User Agent (UA), Message Transfer Agent (MTA), Message Access Agent (MAA), Spool file and Mail Box. These are explained below.

16.2.2.1 User Agent (UA)

The User Agent (UA) is a program. UA provides services to the user which facilitates the sending and receipt of an e-mail message. A typical UA offers the various services to users, such as compose and send a message, to read the incoming message, allow to reply and forward the incoming message. In addition, a UA manages the mailboxes.

16.2.2.2 Message Transfer Agent (MTA)

The Mail Transfer Agent (MTA) is a server program that is basically responsible for transfer of e-mail message from one system to another. MTA realizes recipient’s e-mail address and deliver the e-mail message to the recipient mailbox. In order to send an e-mail, a system needs a client MTA and in order to receive an e-mail, a system needs a server MTA. If both sender and recipient are connected to the same server machine, MTA directly delivers e-mail message to recipient’s mailbox; otherwise MTA of the sender’s server machine transmits e-mail messages to the MTA of destination (say, recipient’s) server machine. Finally, the recipient’s server machine delivers e-mail messages to the recipient’s mailbox. The delivery of an e-mail message from one MTA to another MTA is done through Simple Mail Transfer Protocol (SMTP).

16.2.2.3 Message Access Agent (MAA)

The Message Access Agent (MAA) is a server program which pulls messages from the message store (say, mailbox) and delivers them to the recipient's user agent. The two well known MAA protocols are Post office Protocol, version 3 (POP3) and Internet Mail Access Protocol (IMAP) which are used to retrieve mail from the message store.

16.2.2.4 Spool

A spool is a temporary storage location and is based on queue data structure. Spool kept the e-mails messages on hold until delivery. The e-mail messages are retrieved first in, first out (FIFO) order from the spool by MTA client of sender side server for sending to the MTA server present at the recipient's side server.

16.2.2.5 Mailbox

A mailbox is the storage location of e-mail messages which exist on a remote server. To use e-mail system, each user must have a mailbox that is identified by an email address. Mailbox access is only available to authenticated users. E-mail messages can be downloaded from the mailbox into the user's hard disk. The mailbox keeps all the e-mail messages separately, until deleted by the user. The received e-mail messages are kept in the inbox and the sent e-mail messages are kept in the outbox.

16.3 ARCHITECTURE OF E-MAIL

To explain the architecture of e-mail, a typical scenario is provided, which shown in the figure 2.

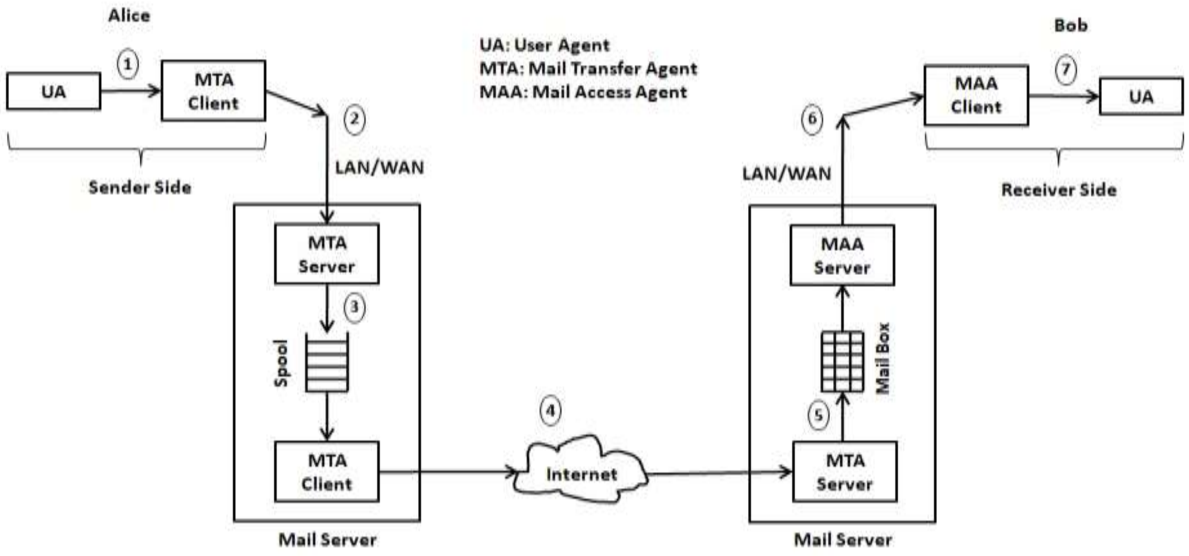


Figure 2: A typical scenario which transmits an e-mail message

Furthermore, the figure 2 depicts the components of the email system. These components are used when Alice sends an email message to Bob.

Step 1: Alice uses the UA to prepare the message.

Step 2: Alice connected to the mail server through LAN/WAN. Thus, she needs MTA client and MTA server to send message. Alice's UA calls MTA client. The MTA client establishes a connection with MTA server, which is running all the time and present in the mail server.

Step 3: The mail server of Alice's site kept all the incoming messages in the spool. The spool is a temporary storage location and is based on queue data structure.

Step 4: The messages are retrieved first in, first out (FIFO) order from the spool by MTA client of Alice's site mail server, then send the messages to the mail server at Bob's site through internet.

Step 5: MTA server present in the Bob's site mail server receives the message and stores in the Bob's mailbox.

Step 6: Bob is also connected to the mail server through LAN/WAN. The Bob's UA calls MAA client and send requests to the MAA server to retrieve messages from the mailbox. The MTA server runs all the time and present in the Bob's mail server.

Step 7: The Bob's UA displays the message.

16.4 PROTOCOLS USED IN EMAIL SYSTEMS

In general, the e-mail system uses three protocols for message communication, such as Simple Mail Transfer Protocol (SMTP), Post Office Protocol, version 3 (POP3), Internet Mail Access Protocol (IMAP). SMTP is a push protocol because it pushes the message from the MTA client to the MTA server. POP3 and IMAP are pull protocols because both protocols pull messages by using MAA client from the MAA server. Figure 3 shows the positions of SMTP, POP3 and IMAP protocols in a typical scenario which transmit an e-mail message from sender to receiver. These protocols are described in brief as follows:

16.4.1 SMTP

The SMTP stands for Simple Mail Transfer Protocol. The SMTP is a client-server protocol that uses port number 25. In general, the SMTP transfers the messages from client MTA to server MTA. In order to send a message, a system must have a client MTA, and for receiving a message, a system must have a server MTA. In order to send a mail, SMTP is used twice. First, SMTP is used between the sender system and the sender's mail server; next, SMTP is used between the two mail servers. For transferring e-mail message, the SMTP employs three phases, i.e. connection establishment phase, mail transfer phase and connection termination phase. SMTP uses commands and responses to transmit the message between an MTA client and MTA server. The commands are sent from MTA client to MTA server and responses are sent from MTA server to MTA client.

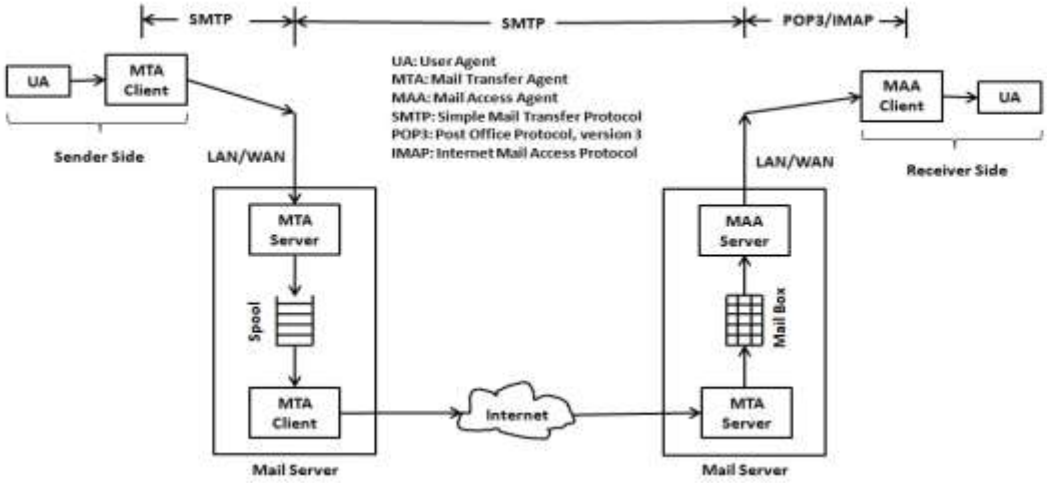


Figure 3: positions of SMTP, POP3 and IMAP protocols

16.4.2 POP3

The POP3 stands for Post Office Protocol, version 3. It is a simple protocol with minimal functionalities, which retrieve e-mail message from mailbox. The POP3 protocol is a client-server protocol, the POP3 client (e.g., MAA client) is installed on the recipient system and the POP3 server (e.g., MAA Server) is installed on the recipient's mail server. A client connects to the server on TCP port 110. The POP3 session has three phases: authorization phase, transaction phase and update phase. In authorization phase, the server verifies the client’s credential and establish the connection. In the transaction phase, the client is allowed to perform various operations (such as, retrieving messages and/or marking messages to be deleted) on the mailbox. During an update phase server delete the messages marked for deletion and terminate the connection. POP3 protocol allows to download the e-mail messages from mail server (say mailbox) to the user's hard disk.

POP3 protocol has several deficiencies. It does not allow the user to create different folders to organize the mail on the server. In addition, POP3 does not allow the user to partially check the contents of the mail before downloading.

16.4.3 IMAP

The IMAP refers to the Internet Message Access Protocol. The IMAP is similar to POP3 and It is also a widely used protocol for retrieving e-mails. Furthermore, IMAP is more complex and more powerful than POP3. It is also based on the client-server model. A client connects to the server through TCP port 143. AMAP provide more features such as, allows to create the folders to organize the e-mails in a hierarchical order; permits to verify the e-mail header before downloading, permission to download the part of the message; makes it possible to create, delete or rename the mailbox on the server; allows to search the e-mails contents using keywords and so forth.

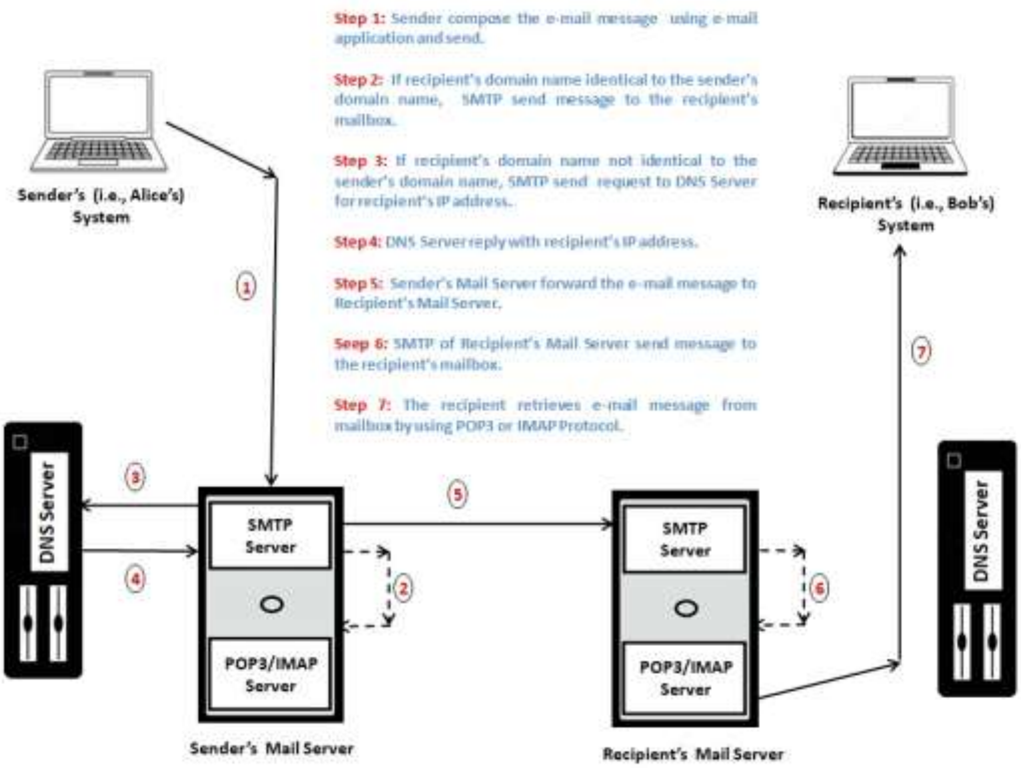
16.5 DIFFERENCES BETWEEN POP3 AND IMAP

POP3 and IMAP are client-server protocols and both are employed to the retrieve the message from the mail server to the recipient's system. The differences between POP and IMAP are as follows:

Post Office Protocol (POP3)	Internet Message Access Protocol (IMAP)
This is a simple protocol with minimal functionalities.	This is a complex protocol with more functionalities than POP3.
It allows you to read the mail only after downloading it.	IMAP allows you to check the mail content before downloading
The POP server listens on port 110.	The IMAP server listens on port 143.
The Message can only be accessed from a single device	The Message can be accessed from multiple devices.
To read the email must be downloaded first onto the local system.	The content of the e-mail can be partially read without downloading.
The user can not organize mails in the mailbox of the mail server.	The user can organize the emails directly on the mail server.
The user cannot create, delete or rename the mailbox on the mail server.	The user can create, delete or rename the mailbox on the mail server.
A user may not search the content of mail before downloading to the local system.	A user may search the content of mail by using keywords before downloading.
Message header can not be viewed prior to downloading.	Message header can be viewed prior to downloading.

16.6 WORKING OF E-MAIL

Email working follows the client server approach. In general the email communication is done via three protocols, such as SMTP, POP3 and IMAP. Suppose Alice wants to send an email message to Bob. The figure 4 describes the path that the email is taken from Alice computer to the Bob's computer. This depicts the way an e-mail is transmitted from sender to receiver.



Step 1: Sender compose the e-mail message using e-mail application and send.

Step 2: If recipient's domain name identical to the sender's domain name, SMTP send message to the recipient's mailbox.

Step 3: If recipient's domain name not identical to the sender's domain name, SMTP send request to DNS Server for recipient's IP address.

Step 4: DNS Server reply with recipient's IP address.

Step 5: Sender's Mail Server forward the e-mail message to Recipient's Mail Server.

Seep 6: SMTP of Recipient's Mail Server send message to the recipient's mailbox.

Step 7: The recipient retrieves e-mail message from mailbox by using POP3 or IMAP Protocol.

First of all, Alice uses an e-mail application to compose the e-mail message. The email message consists the body and the header. The body comprises of the main portion of the message while the header comprises of the subject, e-mail sending date, the sender and recipient address information. The e-mail addresses of Alice's (i.e., sender) and Bob's (i.e., recipient) are alice@example.net and Bob@gmail.com, respectively. When Alice clicks the send button of e-mail application, then the SMTP client delivers the message to its SMTP server, which resides on the Alice site's mail server (i.e., example.net).

The SMTP server, takes the recipient address information from the header and get the domain part of the address to determine the location of the recipient's server. If the recipient's domain name is identical to the sender's domain name, the SMTP merely transfers the e-mail message to the recipient's mailbox. If the recipient's domain name is different from the sender's domain name, the SMTP send a request to the DNS (Domain Name System) server for providing the exact IP address of recipient's domain name's hosted email server. Here, Bob's domain name is gmail.com, which is different from Alice's domain name (i.e., example.net). Hence, the SMTP send a request to the DNS server for Bob's mail server (i.e., gmail.com) IP address.

The DNS server translates the domain names to the IP addresses and vice-versa with the help of Mail eXchange (MX) record. After translation, the DNS server sends a response to the requested mail server (i.e., Alice's mail server). The DNS server response message contains the IP address of the recipient's mail server (i.e., Bob's mail server).

Next, the e-mail message is transmitted between the mail servers. After receiving the recipient's mail server IP address from the DNS server, the sender's mail server (i.e., Alice's mail server) forward the message with the help of the SMTP client.

The recipient's mail server (i.e., Bob's mail server) receive the e-mail message with the help of the SMTP server. Furthermore, the SMTP server will store the e-mail message in the recipient's mailbox (i.e., Bob's mailbox) and make it available to the recipient (i.e., Bob).

The recipient (i.e., Bob) retrieves e-mail message from mailbox by using an e-mail application. The e-mail application may use either POP3 or IMAP client-server protocol. In general, the POP3 client or IMAP client is present at the recipient's (i.e., Bob) e-mail application, whereas the POP3 server or IMAP server is present at the recipient's mail server (i.e., Bob's mail server).

16.7 TYPES OF E-MAIL

The brief description of different types of e-mail's are as follows:

Newsletters: this is the most common type of e-mail that are sent on a consistent schedule (either daily, weekly, or monthly) to all subscribers of the mailing list. Typically, Newsletter e-mails convey important information to their client through a single source that often contain businesses offering, upcoming events, news, certain blog or website and so on.

Lead Nurturing: Lead nurturing is the technique used to establish a relation between brands and consumers. This relationship building takes place through the sales funnel, from user's first inquiry to making a purchase. A lead nurturing e-mail campaign is an automated, personalized, e-mail campaign, usually sent in several days or weeks, that may affect the purchasing behavior of users. Furthermore, lead-nurturing e-mails are initiated by the potential buyer who takes initial steps, such as clicking on links to a promotional e-mail or downloading complimentary sample.

Promotional e-mails: This is the easy way to educate potential customers on new and existing products or services. Promotional e-mail include coupons or discount offer, access to exclusive content, or invite to attend an event. These types of e-mails are sent to new or existing customers with a limited time offer, hence they take immediate action, such as purchase product, avail the service, and so on.

Standalone e-mails: These e-mails are precisely on one topic, with the intention that readers' attention is not distracted, so that they are more likely to take the steps you want them to take. The standalone e-mails are characterized by any one topic, such as advertising content, brand messages, sign up for the webinar, to buy a particular product, to read the latest blog post of a particular person, consent to receive information bulletin via e-mail and so forth.

Onboarding emails: The onboarding e-mails are transmitted to buyers to acquaint and train them to effective use of the product. It is also known as after-sales e-mails that is used to enhance customer loyalty. The onboarding e-mail make new user habits, convert free users into paying subscribers, and build long-term engagement.

Transactional: This e-mail is sent automatically from a sender to a recipient, when the recipient has completed a business transaction or account activity in an application/website. Transactional e-mail often contains valuable information to the customer. Examples of transactional e-mail are purchasing receipts, shipping notification, personalized product notifications, password resets, etc.

Plain-Text e-mails: This is a simple e-mail message which contains text only. The plain-text e-mails are unformatted and the absence of graphics or images. The plain text e-mails can be typically used for sales letters, leave application, blog content, event invitations, survey or feedback requests.

16.7.1 Advantages of e-mail

There are many benefits of e-mail, and these are:

- **Cost-effective:** E-mail is a very cost-effective service (almost free) that allows you to communicate with other people.

- **Accessible anywhere and anytime:** E-mail enables users to access messages from anywhere and anytime through an Internet connection.

- **Speed and simplicity:** E-mails can be easy to compose and immediately delivered to the recipient.

- **Mass sending:** In a short time an e-mail can be sent to many people.

- **Future retrieval:** E-mail exchanges are saved and can be retrieved a particular message in feature by searching.

- **Message categorization:** E-mail provides a simple user interface and categorize messages, so users can easily find specific messages. Additionally, it can help the user to recognize unwanted e-mails such as junk and spam mail.

- **Eco-friendly:** E-mail reduces paper consumption and contributes to saving the environment.

16.7.2 Disadvantages of Email

There are numerous disadvantages to email, and these are:

- **Malicious Use:** Anyone who has usernames, passwords and an email address can send an email. Some instances, an unauthorized person fraudulently obtains usernames, passwords of a specific person and send emails to groups of people to spread gossip or misinformation.

- **Message overwhelming:** There are unsolicited advertising and unwanted messages arriving through e-mail, which cause overwhelming messages.

- **Virus Carrier:** The viruses can get into the system in numerous ways and infect it. One common way to enter viruses is through e-mail. In some cases, the virus is accompanied by a document or link attached to the email. The virus may infect the system when recipients click on the e-mail and open the attached document/link.

- **Cyber threats:** E-mail is the gateway to most of cyber threats. An email attack occurs when a malicious actor targets a particular person's e-mail id with the intention of illegally accessing the system, channelling money, obtain sensitive information such as confidential document or personal messages.

16.8 E-MAIL ATTACK

E-mail is one of the most widely used techniques for message communication. It is utilized by individuals to stay connected with friends and family members. Moreover, almost all business and banking organizations also use e-mail messaging services, such as online purchase confirmations, bank account statements, and so on. As many people in the globe depends on the e-mail, it has become one of the main techniques employed by the cyber criminal.

An email attack may be described as an event in which the email is used to damage or harm an individual or an organization. Although the way of email-based attacks are different, but the goal of cyber criminals is to steal money or data. In order to preserve e-mail security, it is important that everyone need to be aware of the most common types of email attacks and realize their potential impact.

16.8.1. Spam

Spam is the most commonly known form of email attack and it is an unsolicited e-mail. Cyber criminals send spam emails in bulk to several victims at once. More often Spam e-mails are likely to repeat multiple times (as long as the cyber criminal runs his or her campaign). Spam e-mails are some extent harmless, but more often, spam is used for laying the groundwork for launching other types of email attacks such as spear phishing. Spam e-mail usually contains harmful links, malware or deceptive content. Spam mails are different from the promotional e-mail form companies. The receiving of promotional e-mail can be stoped by just unsubscribe to these e-mails, but Spam e-mail does not stop by unsubscribing. The end goal is to obtain sensitive information such as a social security number or bank account information. Most spam comes from multiple computers on networks infected by a virus or worm. These compromised computers send out as much bulk email as possible.

Safety tip: Ignoring spam is the best policy, and setting up spam filters on e-mail works best.

16.8.2 Phishing Attacks

Phishing is a fraudulent attempt to obtain sensitive information such as usernames, passwords and credit card details by pretending to be a trusted entity. In phishing attacks, cyber criminals are sent the legitimate look e-mail to many users. The purpose of the message is to encourage the receiver to install malware on their device or to share personal or financial information. In general, the phishing emails are not personalized and tend to start with generic greetings like "hello" or "dear sir" and so on. In phishing attacks, lucrative offers mentioned in the email subject lines to lure the victim. Furthermore, the victim is asked to click a link and fill out a form on a phishing website, to capture the credentials. From the mere number of people receiving the email, even if a small percentage of targets fall on the attack means that the attacker is likely to have a certain success.

Safety tip: Never download untrusted email or website attachments. Moreover, don't share the personal or financial information in any website for lucrative offer.

16.8.3 Spear phishing

Spear phishing is an advanced phishing attack. Spear phishing targets one or a few people in particular and tries to impersonate a trustworthy person or entity. In the spear phishing attack, the cyber criminals spend some time for researching the target's interests before sending the email. In order to make the email appear legitimate the attacker sends customized emails. In general, spear phishing emails are more sophisticated in their construction and convincing in execution, they are harder to catch.

Safety tip: Never download unreliable email enclosures. As well, do not visit or share personal information on an unreliable website or social site.

16.8.4 Whaling Email Attack

A whaling email attack is a special form of email fraud that has successfully tricked users into revealing sensitive business information and transferring millions of dollars to fraudulent accounts. A whaling email is a form of phishing where hackers send a message that appears to be from a chief executive officer, the chief financial officer or another top class executive. To create a whaling email, attackers will research a targeted individual, usually collecting personal information from online profiles and social media accounts. A whaling email is much more difficult to spot than a regular phishing attack. The design of a whaling email will look identical to an email from a legitimate source, usually someone the recipient knows and trusts. The sender's email address in a whaling email may be slightly altered from the domain name of a legitimate or trusted company. For example, an email from "name@acme.com" may be substituted with "name@acrne.com", where the "m" in the original domain is replaced with "rn" that is difficult for a casual observer to spot. Often, a whaling email will have an urgent or a slightly threatening tone that's intended to encourage the recipient to act quickly and without taking time to confer with others or double-check information. The purpose of a whaling email is to trick the recipient into revealing sensitive information that attackers can use to steal data, or to transfer of funds to a fraudulent account. The content of a whaling email may ask the recipient to transfer money to a vendor or a bank account, to email sensitive data like tax information or payroll files to a spoofed email address, or to visit a spoofed website where the target is asked to enter sensitive information like passwords or bank account numbers. Visiting such a website may also enable attackers to download malware to the victim's computer.

Safety tip: To stop a whaling cyber attack, need to scans of all inbound email to examine the anomalies in the display name, domain name, recency of the domain. On reply-to information and the body of the message looks for certain words and phrases like "wire transfer", "bank transfer" or "W-2" that may indicate a whaling cyber attack.

16.8.5 Virus

Viruses may spread by email. A virus is a type of malicious code or program that spreads from host to host with the capability of replication. Viruses often hide behind e-mail attachments such as a text message, program file, image, greeting card, audio file, video file, and so on. In general, user interact with e-mail and download the file to the machine at that time virus get deployed through the batch files. When the user run the infected file or program, which in turn causes the virus code to be executed. The virus could quickly spread across the computer system in a short time and can even have the ability to steal passwords or data, log keystrokes, corrupt files and so on. Some viruses are designed to carry out damaging effects such as erasing data or causing permanent damage to the computer hard disk. Some viruses are designed with a view to financial gains. The virus can spread from an infected computer to other computers within the same network and eventually damage the entire network.

Safety tip: Viruses typically reside in word or other office documents. To avoid contact with a virus and stay safe, never download text or email attachments that you're not expecting, or files from websites you don't trust.

16.8.6 Pharming

In pharming attack, the attacker misdirects users to a fake website that appears to be official. The fake websites are created by attacker for the purpose of stealing personal information. Once redirected to these fake websites, users are prompted to enter personal information, which is then used to commit identity theft or financial fraud. The pharming attack is done by either infiltrating individual computers or DNS cache poisoning. In the infiltrating individual computer type pharming, the hacker sends an email with a code that modifies the host files of an individual's computer. In general, a computers maintains a list of previously-visited websites and IP addresses in a locally-stored "hosts" file. Once the host files are infiltrated, they can redirect URLs to a fake version of the website the individual is intending to visit. Even if the user types in the correct URL, the page will redirect. These websites mimic the appearance of real sites so users may not be aware they are victims. The DNS cache poisoning is an older method of pharming. When a user wishes to visit a URL via their internet browser, the browser contacts the DNS server to request the IP address for the desired domain. Each DNS server has maintained its own set of listings or listings obtained from others in the DNS table, or cache. In DNS cache poisoning attack, the attacker rewrites the DNS table, or cache so that user's URL request redirecting to the IP address of their spoofed website without the user’s knowledge or consent. The DNS cache poisoning event has the potential to affect multiple users at once.

Safety tip: **Check to make sure the URL is spelled correctly, Be sure the URL is secure and has “https” before the site name. If you think you are a victim of an attack, clear your DNS cache. If you believe your server is compromised, contact your Internet service provider. Install a VPN for secure online browsing.**

16.8.7 Ransomware

Ransomware attack is a type of malware attack and it can enter the systems through an email. Ransomware attacks are usually carried out with the help of a Trojan horse disguised as a legitimate file that the user is tricked into downloading or opening when it arrives as an email attachment. In Ransomware attack, attacker encrypts the victim’s important, predetermined files with a password and making them inaccessible. Finally, attacker leave a note as a text file, demands money (usually, Bitcoin cryptocurrency) in return for the decryption key.

Safety tip: **Do not download irrelevant attachments from an e-mail or website. In addition, periodically take the back up of important files and documents.**

16.8.8 Spyware

Spyware is a program that enables a criminal to obtain information about a user’s computer activity and sends it over the internet without user knowledge. This information is generally obtained through cookies and the history of the web browser. In addition, to get the information Spyware often includes activity trackers, keystroke gathering, and data capture. Spyware may also install other software, display ads, or reroute web browser activity. In an effort to overcome security measures, spyware normally changes security settings. Spyware often gets carried away with legitimate e-mail, software or Trojan horses.

Safety tip: Never download irrelevant files from an e-mail. Scan the software prior to installation as well as downloading from the website. Furthermore, delete cookies and browser history from time to time.

16.8.9 Business Email Compromise (BEC) Attacks

In an BEC attack, an attacker tries to convince a person or organization to believe that it is a reliable contact before stealing money or information.In such attacks, the attacker targets companies that tend to process payments remotely and off-site. An attacker patiently monitors the user's e-mail communication and checks the way the e-mail is handled. Then, in due course, the attacker presents himself or herself as a trustworthy individual or organization and often engages in a conversation through multiple emails, before requesting for payments, credentials or confidential data. This type of attack uses neither links nor attachments to deploy malicious code.

Safety tip: Encryption of e-mail reduces the risks associated with data loss and corporate policy violations while allowing crucial business communications. For protection of sensitive data, encrypt the file before sending it by email. At the end of the recipient, the end user will decrypt the file and read the contents of the file.

16.8.10 Account Take Over (ATO) Attack

In ATO attack, an attacker actor gains unauthorized access to an account belonging to someone else. In such an attack, the aim of the cybercriminal is to collect personally identifiable information that will be used in other forms of fraud and identity theft. In this type of attack, the cyber criminals spend time for researching across open databases and social media, looking for relatable information like name, location, phone number, or names of family members, and so on – anything that will help in guessing a password. Once the attacker has identified valid credentials for a user account, then the attacker can change account details, send out phishing emails, steal financial information or sensitive data, or use any stolen information to access further accounts. Sometime, the attacker sells the working login credentials to others. Often, data taken from an account leads to more ATO and other forms of cyber-attacks.

Safety tip: Use the distinct passwords for separate accounts. Change your passwords from time to time.

16.9 E-MAIL SECURITY

Email allows individuals to communicate with each other. It also provides an opportunity for members of organizations to communicate with each other as well as with members of other organizations. The e-mail was designed to be as open and approachable as possible. As email is an open format, it is available to anyone who can intercept it, which causes security problems. Attackers try to take advantage of the lack of email security to make money by performing their actions, such as read the contents of an email, spam campaigns, malware and phishing attacks, sophisticated targeted attacks, or business email compromise (BEC). The security of emails is therefore an important concern.

E-mail security is a term for describing different procedures and techniques for protecting sensitive information in email communication, user accounts against unauthorized access, spam filtering, data loss or compromise, e-mail encryption, and so on. E-mail security is needed for the holder of an individual e-mail account and a professional organisation. There are many steps that individuals and organizations should take to improve the safety of emails.

16.9.1 Organization Email Security Best Practices

There are some important practices that organization should follow to ensure secure usage of e-mail.

- Make sure webmail applications are able to secure logins and use email encryption technique to protect both email content and attachments.

- Implement a data protection solution to identify sensitive data and prevent them from being lost through e-mail.
- Defend malicious attachments using multiple signature-based, static and sandboxing inspections.
- Block viruses and spam through a strong and secure e-mail gateway. Implement scanners and other tools to analyze messages and block emails containing malware or other malicious files before they reach your end users.
- Use anti-malware and anti-spam protection which can prevent some attacks from reaching users' mail boxes.
- Block an advanced mail attack like impersonation or phishing attacks with real-time scanning of all inbound emails.
- Stop internal attacks through data loss prevention protocol (DLP) and content control capabilities by scanning incoming and outgoing emails in real time.
- Use email scanning and archiving technology to neutralize ransomware attacks.The mail administrator should back up the mail server on a regular basis to archiving of data and information, including those found in e-mail.
- Protect against malicious links through URL analysis. Email security software that analyzes and filters each link and attachment within each email, preventing users from accessing URLs or opening attachments that can be malicious.
- Prevent spoofing with *Domain Name System* (*DNS*) authentication services, which uses SPF (Sender Policy Framework), DKIM (DomainKeys Identified Mail) and DMARC (Domain-based Message Authentication, Reporting & Conformance) protocols to identify legitimate and potentially fraudulent email.
- when the company enables employees to access company emails on personal devices Implement security best practices for Bring Your Own Device (BYOD).
- Educate employees about email security through security awareness training. The training programme educates the employee about how to avoid being victimized by various types of email attacks, realization of appropriate steps to secure e-mail, and how to prevent sensitive data loss or malware infections via email.

16.9.2 Individual User Email Security Best Practices

There are some important practices that individual users (organization employees) should follow to ensure secure usage of e-mail.

- Use est practices to create strong passwords and regularly modify the password.
- Never share your passwords with anybody, including your colleagues and friends.
- Use spam filters and antivirus software prior to downloading and uploading files.
- Never open attachments or click on hyperlinks in emails received from unknown senders.
- Try to send as little sensitive information by e-mail, and only send encrypted sensitive information by e-mail to recipients who need it.
- Do not access corporate emails from public WiFi connections.

- If an employee of the organization is working remotely or on a personal device, use the Virtual Private Network (VPN) software to access the company's e-mail.

16.10 EMAIL ATTACKS AND CRIMES

Email crimes or attacks can be a direct one where users can use them to harass or intimidate a receiver. There exist lots of crimes which are perpetrated directly using emails. Also email attacks can be indirect where emailing is used as one of the tool to capture sensitive information and perform malpractices or induce malwares into the client system. Let us look into few email attacks or crimes.

1. **Flaming**
2. **Email spoofing**
3. **Email bombing**
4. **Email hacking**
5. **Spams**
6. **Email frauds**
7. **Email phishing**

16.10.1 Flaming

Flamming occurs when a person sends a message with angry or antagonistic content. The term is derived from the use of the word Incendiary to describe particularly heated email discussions. Flaming is assumed to be more common today because of the ease and impersonality of email communications: confrontations in person or via telephone require direct interaction, where social norms encourage civility, whereas typing a message to another person is an indirect interaction, so civility may be forgotten.

16.10.2 Email spoofing

It occurs when the email message header is designed to make the message appear to come from a known or trusted source. Email spam and phishing methods typically use spoofing to mislead the recipient about the true message origin.

16.10.3 Email bombing

It is the intentional sending of large volumes of messages to a target address. The overloading of the target email address can render it unusable and can even cause the mail server to crash.

16.10.4 Email hacking

It is illicit access to an email account or email correspondence.

16.10.5 Spams

Attackers often send massive email broadcasts with a hidden or misleading incoming IP address and email address.Some users may open the spam, read it, and possibly be tempted by whatever wares or schemes are offered.

16.10.6 Phishing

This type of attacks uses email messages from legitimate businesses that the user may be associated with. Although the messages look authentic with all the corporate logos and similar format as the official emails, they ask for verification of personal information such as the account number, password, and date of birth. 20% of unsuspecting victims respond to them, which may result in stolen accounts, financial loss and identity theft.

16.10.7 Email fraud

It is the intentional deception made for personal gain or to damage another individual through email. Almost as soon as email became widely used, it began to be used as a means to defraud people. Email fraud can take the form of a "con game" or *scam*. Confidence tricks tend to exploit the inherent greed and dishonesty of their victims. The prospect of a 'bargain' or 'something for nothing' can be very tempting. Email fraud, as with other 'bunco schemes' usually targets naive individuals who put their confidence in get-rich-quick schemes such as 'too good to be true' investments or offers to sell popular items at 'impossibly low' prices. Many people have lost their life savings due to fraud.

16.10.8 Phishing emails

It may contain links to websites that are infected with malware.Phishing is typically carried out by email spoofingor instant-messaging,and it often directs users to enter details at a fake website whose look and feel are almost identical to the legitimate one. Phishing is an example of social engineering techniques used to deceive users, and exploits the poor usability of current web security technologies.

16.11 PRIVACY IN EMAILS

16.11.1 Email privacy

It is the broad topic dealing with issues of unauthorized access and inspection of electronic mail. This unauthorized access can happen while an email is in transit, as well as when it is stored on email servers or on a user computer. In countries with a constitutional guarantee of the secrecy of correspondence, whether email can be equated with letters and get legal protection from all forms of eavesdropping comes under question because of the very nature of email. This is especially important as more and more communication occurs via email compared to postal mail.

Email has to go through potentially untrusted intermediate computers (email servers, ISPs) before reaching its destination, and there is no way to tell if it was accessed by an unauthorized entity. This is different from a letter sealed in an envelope, where by close inspection of the envelope, it might be possible to tell if someone opened it. In that sense, an email is much like a postcard whose contents are visible to everyone who handles it.

There are certain technological workarounds that make unauthorized access to email hard, if not impossible. However, since email messages frequently cross nation boundaries, and different countries have different rules and regulations governing who can access an email, email privacy are a complicated issue.

A significant fraction of email communication is still unencrypted. In general, encryption provides protection against malicious entities. However, a court order might force the responsible parties to hand over decryption keys;

- Email privacy, without some security precautions, can be compromised because:
- Email messages are generally not encrypted.
- Email messages have to go through intermediate computers before reaching their destination, meaning it is relatively easy for others to intercept and read messages.
- Many Internet Service Providers (ISP) store copies of email messages on their mail servers before they are delivered. The backups of these can remain for up to several months on their server, despite deletion from the mailbox.
- The "Received:"-fields and other information in the email can often identify the sender, preventing anonymous communication.

16.11.2 Email tracking

It is a method for monitoring the email delivery to intended recipient. Most tracking technologies use some form of digitally time-stamped record to reveal the exact time and date that an email was received or opened, as well the IP address of the recipient.

Email tracking is useful when the sender wants to know if the intended recipient actually received the email, or if they clicked the links. However, due to the nature of the technology, email tracking cannot be considered an absolutely accurate indicator that a message was opened or read by the recipient.

10.12 SUMMARY

1. **An email message consists of two main sections: the header and the body.**
2. **A typical e-mail header contains the** *From*, *To*, *Subject* **and** *Date.*
3. **Email addresses are always made up of a username followed by a @ sign and a domain name. For instance, username@domainname.**
4. **The body of the message contains the information that the recipients have to read.**
5. **The basic components of an e-mail system are: User Agent (UA), Message Transfer Agent (MTA), Message Access Agent (MAA), Spool file and Mail Box.**
6. **The Mail Transfer Agent (MTA) is a server program that is basically responsible for transfer of e-mail message from one system to another.**
7. **The delivery of an e-mail message from one MTA to another MTA is done through** Simple Mail Transfer Protocol **(SMTP).**
8. **The Message Access Agent (MAA) is a server program which pulls messages from the message store (say, mailbox) and delivers them to the recipient's user agent.**
9. **The two well known MAA protocols are Post office Protocol, version 3 (POP3) and Internet Mail Access Protocol (IMAP).**
10. **A mailbox is the storage location of e-mail messages which exist on a remote server.**
11. **the e-mail system uses three protocols for message communication, such as Simple Mail Transfer Protocol (SMTP), Post Office Protocol, version 3 (POP3), Internet Mail Access Protocol (IMAP).**
12. **SMTP employs three phases, i.e. connection establishment phase, mail transfer phase and connection termination phase.**
13. **SMTP uses commands and responses to transmit the message between an MTA client and MTA server.**
14. **The POP3 session has three phases:** authorization **phase,** transaction **phase and** update **phase.**
15. **The DNS server translates the domain names to the IP addresses and vice-versa with the help of Mail eXchange (MX) record.**
16. **An email attack may be described as an event in which the email is used to damage or harm an individual or an organization.**

10.13 CHECK YOUR PROGRESS

1. SMTP is a simple

   a) TCP protocol
   b) UDP protocol
   c) IP protocol
   d) None of the above

2. A simple protocol used for fetching e-mail form a mailbox is

   a) CIMP

b) POP3
c) SMTP
d) None of the above

3. E-mail address is made up of

a) Single part
b) Two parts
c) Three parts
d) Four parts

4. SMTP stands for

a) Short Mail Transmission Protocol
b) Small Mail Transmission Protocol
c) Server Mail Transfer Protocol
d) Simple Mail Transfer Protocol

5. E-mail addresses separate the user name from the ISP using the ________ symbol.

a) &
b) $
c) @
d) %

Answers:

1. (a)
2. (b)
3. (b)
4. (d)
5. (c)

10.14 MODEL QUESTIONS

1. **Write the some important best practices that organization should follow to ensure secure usage of e-mail.**
2. **Write the some important best practices that individual users (organization employees) should follow to ensure secure usage of e-mail.**
3. **Describe the structure of SMTP messaging with a neat diagram.**
4. **Which headers in SMTP useful in tracing a message sender identity?**

5. List and describe atleast 4 email attacks.
6. How is privacy a big issue in emailing?
7. What are the various types of email services?

10.15 FURTHER READINGS

1. Debra Littlejohn Shinder, Michael Cross, Scene of the Cybercrime, syngress
2. Linda Volonino, Reynaldo Anzaldua; Computer Forensics For Dummies, Wiley Publishing, Inc.
3. Gutiérrez, Carlos A., Web Services Security Development and Architecture: Theoretical and Practical issues, IGI Global, 2010.

References, Article Source & Contributors

[1] Email - Wikipedia, the free encyclopedia, https://en.m.wikipedia.org/wiki/Mail_headers

[2] Email privacy - Wikipedia, the free encyclopedia, https://en.wikipedia.org/wiki/Email_privacy

[3] Email tracking - Wikipedia, the free encyclopedia, https://en.wikipedia.org/wiki/Email_tracking

[4] E-mail: Message Format | World4Engineers, world4engineers.com/e-mail-message-format/

[5] EMailTracer, http://www.cyberforensics.in/OnlineEmailTracer/index.aspx

[6] M. Tariq Banday, Techniques and Tools for Forensic Investigation of E-Mail, International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.6, November 2011

[7] Phishing - Wikipedia, the free encyclopedia, https://en.wikipedia.org/wiki/Phishing

EXPERT PANEL

Dr. Jeetendra Pande, Associate Professor- Computer Science, School of Computer Science & IT, Uttarakhand Open University, Haldwani

Dr. Ajay Prasad, Sr. Associate Professor, University of Petroleum and Energy Studies, Dehradun

Dr. Akashdeep Bharadwaj, Professor, University of Petroleum and Energy Studies, Dehradun

Mr. Sridhar Chandramohan Iyer, Assistant Professor- Universal College of Engineering, Kaman, Vasai, University of Mumbai

Mr. Rishikesh Ojha, Digital Forensics and eDiscovery Expert

Ms. Priyanka Tewari, IT Consultant

Mr. Ketan Joglekar, Assistant Professor, GJ College, Maharastra

Dr. Ashutosh Kumar Bhatt, Associate Professor, Uttarakhand Open University, Haldwani

Dr. Sangram Panigrahi, Assistant Professor, Siksha 'O' Anusandhan, Bhubaneswar

This MOOC has been prepared with the support of