E-mail and Instant Messaging

Chapter 16

Security of E-Mail Transmissions

- E-mail –
  - The most popular application on the Internet and the intranet
  - Users should secure e-mails as they send and receive the messages.
  - Security administrators can provide users the tools to fight security problems.
- Server-based and desktop-based virus protection
  - help block malicious code,
- spam filters
  - help block unsolicited commercial e-mail.

Malicious Code

- Viruses/worms spread faster by e-mail.
- **Worms**
  - Scripted to send themselves to other users.
  - Uses its code to automate the infection process.
  - Use multiple methods of attack, which include:
    - Sending multiple infected e-mails.
    - Scanning hosts on the Internet, looking for a specific vulnerability.
    - Finding the vulnerability and infecting the target.
  - Endanger individual systems and network security
    - Introduce malicious traffic to other machines.
  - Causes a loss of data and potentially discloses private data.

Trojan Horse

- A Trojan horse
  - A program that seems to be one thing while actually having a hidden purpose.
  - They **may do what they claim**, but they also install some other program that allows an attacker to control an infected machine remotely.
  - Once control is achieved, the attacker can use the machine to perform any number of tasks.

Malicious Code – HTML

- Hypertext Markup Language (HTML)
  - Allows plain text to represent complex page designs.
  - It was adopted by e-mail programs so users could use different fonts, colors, and pictures in their e-mails.
- Some e-mail programs have a preview pane
  - Enables users to read e-mails without opening them in full screen.
  - This preview activates all the content in the e-mail message.

Malicious Code – HTML

- Users need not run the program or open the e-mail to activate the worm
  - They just need to view the e-mail in the preview pane.
- Viruses are a security threat.
  - One of the most common transfer methods is through e-mail.
  - This threat can be reduced by educating the users and scanning for viruses.
  - Most users are aware of viruses and the damage they cause.
    - They need to be briefed about specific activities when the virus comes through e-mail.

Malicious Code – Good Practice

- Examine all e-mails for a known source and destination, especially if the e-mails have attachments.
- Check strange files or unexpected attachments.
- Recognize:
  - Viruses may be executed by opening the e-mail or viewing it in the preview pane.
- Education and proper administration
  - Also useful in configuring the e-mail software to be as virus-resistant as possible.
- Have a well thought out virus-scanning procedure
  - Perform virus scanning on every e-mail as it enters the organization's server.
  - Some users attempt to retrieve e-mail from their normal off-site ISP account. This may bypass the server-based virus protection.
- Use host-based virus protection programs.
  - Scan all files on a regular basis and perform checks on files upon execution

Important

Hoax E-Mails

- E-mail hoaxes are a nuisance.
  - An e-mail hoax is a global urban legend traveling from one e-mail account to the next.
  - Most have a common theme of some story that must be told right away or some virus that everyone should beware.
  - Cost everyone not only in the time wasted by receiving and reading the e-mail, but also in the Internet bandwidth and the server processing time.

Unsolicited Commercial E-Mail (Spam)

- Spam is the common term for unsolicited commercial e-mail.
- The appeal of spam is the extremely low cost per advertising impression.
  - Senders can send their messages for less than a cent apiece.
- Less expensive than traditional direct mail or print advertisements.
  - The low cost ensures the continued growth of spam e-mail unless something is done.

Unsolicited Commercial E-Mail (Spam)

- The amount of spam is large enough to trigger state and federal legislators to consider action.
  - No effective laws have been passed and this has forced most people to seek technical solutions to the spam problem.
- One way to fight spam is to be cautious about where to post e-mail addresses.
  - Users cannot keep e-mail addresses secret just to avoid spam.
  - One of the steps many system administrators of Internet e-mail servers have taken to reduce spam **is to shut down mail relaying**.

Unsolicited Commercial E-Mail (Spam)

- It is not possible to close all mail relays.
  - Spammers will mail from their own mail servers.
- Software must be used at the recipient's end to combat spam.
- Spam can be filtered
  - at the host level with pattern matching, focusing on the sender, the subject, or the text of the e-mail.
  - at the server level by using pattern matching, but some mail software also use the Realtime Blackhole List. This list is maintained for blocking spam mail.
- Other methods
  - Commercial packages that block spam at the server level using both the methods by maintaining their own blacklists and pattern-matching algorithms.

Fighting Spam

- Ways to fight spam include:
  - E-mail filtering
  - Educate users about spam
    - Cautious internet surfing
    - Cautious towards unknown e-mail
  - Shut down open relays
  - Host/server filters
  - Blacklisting

Mail Encryption

- E-mail has always been a plaintext protocol.
  - E-mail is sent with the clear text of the message exposed to anyone who is sniffing the network.
  - Any attacker at a choke point in the network could read all e-mails passing through that network segment.
- E-mails must be encrypted to solve problems associated when sending them.
- They can be encrypted using:
  - S/MIME
  - PGP

Secure/Multipurpose Internet Mail Extensions (S/MIME)

- S/MIME
  - A secure implementation of the MIME protocol specification.
  - Encode the message in one of the two ways:
    - The host mail program can encode the message with S/MIME.
    - The server can act as the processing agent, encrypting all messages between hosts.
  - The host-based operation starts when the user clicks Send.
  - The mail agent encodes the message using the generated symmetric key.
  - The symmetric key is encoded with the remote user's public key or the local user's private key.
    - This enables the remote user to decode the symmetric key and then decrypt the actual content of the message.

All this is handled by the user's mail program.

Important

S/MIME

- If the message is signed by the sender, it will be signed with the sender's public key, guaranteeing the source of the message.
- Symmetric and asymmetric encryption are used in e-mails to increase the speed of encryption and decryption.
  - As encryption is based on difficult mathematical problems, it takes time to encrypt and decrypt.
  - To expedite this, asymmetric encryption is used to encrypt only a relatively small amount of data, the symmetric key.
  - The symmetric key is then used to encrypt the rest of the message.

Important

S/MIME

- If the message is signed, the S/MIME process of encrypting e-mails provides
  - integrity,
  - privacy,
  - and authentication.
- Some of the problems with its implementation are:
  - S/MIME allows the user to select low strength (40-bit) encryption.
  - The user can send a message that is thought to be secure but that can be more easily decoded than messages sent with 3DES encryption.
  - There may be flaws in software.

Important

PGP

- Pretty Good Privacy (PGP)
  - Implements e-mail security in a similar way to S/MIME using different protocols.
  - The user sends the e-mail, and the mail agent applies encryption as specified in the mail program.
    - The content is encrypted with the generated symmetric key.
    - That key is encrypted with the public key of the recipient of the e-mail, or with the private key of the sender.
  - Senders can also sign the mail with their private key, allowing the recipient to authenticate the sender.
  - PGP supports Public Key Infrastructure (PKI) provided by multiple vendors, including X.509 certificates and LDAP key sources such as Microsoft's Active Directory, and Novell's NDS.
  - PGP generates its own keys.
    - It transmits the public keys to the PGP LDAP server

Important

Decoding PGP - Eudora

- The program does not decrypt the message upon receipt. It waits until instructed to do so.
- PGP stores encrypted messages in the encrypted format, as S/MIME.
  - It provides end-to-end security for the message.