Chapter: 11.2 Overview of Internet Security

Topic: 11.2.3 E-mail threats and Secure E-mail

E-mail threats and Secure E-mail

- E-mail when sent across the internet is more like a post card.
- It can be intercepted at any stage and read by anybody who can lay his hands on it.
- To ensure the secrecy of the message, the sender as well as the receiver should agree on the secret key.
- There starts the problems, if user's intended recipient is in faraway country, then user have to distribute the key first to him before user can send him the message.
- And it presents a logistical problem, Public key cryptography was designed to overcome this problem through what is known as public key private key pair.
- Another way to ensuring the secrecy of the e-mail messages is through the use of a technique called singing a message.

Web security and Privacy concepts

- The control panel of our system provides us with 'Internet options' where we can set the level of privacy and security of our web browsers.
- Using 'security options', user can block certain unwanted and unsecure sites.
- Using 'privacy option', user can select the zone for blocking cookies as per the requirements.

What are cookies?

- The term "cookie" is derived "magic cookie", a well-known concept in UNIX computing.
- In simple computing terms a cookie is a small string of text stored on a user's computer by a web browser.
- Cookie is a message given to a web browser by a web server which is stored by the browser in a text file.

- The message is then sent back to the server each time the browser request a page from the server.

- The main purpose of cookies is to identify users and possibly prepare customized web pages for them.

- Websites use cookies for different reasons:

  ➢ To collect demographic information about who is visiting the web site.

  ➢ To personalize the user's experience on the web site cookies help to store personal information about you so that when you return to the site you have a more personalized experience.

  ➢ To monitor advertisements.

- Thus cookies are text files that can be deleted at any time.

- They cannot be used to spread virus and can't access your hard drive.

- Cookies do not act maliciously on computer systems.

The Simple Network Management Protocol

- The simple network management protocol is a frame work for managing devices in an internet using the TCP/IP protocol suite.

- It provides a set of fundamental operations for monitoring and maintaining on internet.

- The SNMP uses the concept of a manager and agent.

- A manager is a host that runs the SNMP client program.

- A manager is a host that runs the SNMP server program.

- Management is done through simple interaction between manager and agent.

- The agent keeps performance information in a database.

- The manager has access to value in the database.

- SNMP is an application level protocol in which a few manager stations control a set of agents.

- The protocol is designed at the application level so that it can monitor devices made by different manufacturers and installed on different physical networks.

- SNMP frees the management tasks from both the physical characteristics of the managed devices and underlying networking technology.

- Management with SNMP is based on three basic ideas:
  - ➢ A manager checks an agent by requesting information that reflects the behavior of the agent.
  - ➢ A manager forces an agent to perform a task by resulting values in agent database.
  - ➢ An agent contributes to the management process by warning the manager of an unusual situation.

Role of SNMP

- SNMP has some very specific roles in network management.
- It defines the format of the packet to be sent from a manager to an agent.
- It also interprets the result and creates statistics.
- The packets exchanged contain the object variable names and their status (values) SNMP is responsible for reading and changing these values.

VPN

- Virtual private network allows a computer to connect to a corporate LAN over the internet.
- Virtual private network is an extremely important technology that is in wide spread use.
- A VPN is carried over a shared or public network which is almost always the internet and encrypts the message so that only the VPN client and server can access it.
- The cost of VPN connections are much less than dedicated connections such as WAN technologies because they take advantage of the art efficiency of the Internet without compromising security.

VPN Connections

- These connections are used in two important ways:
  - ➢ To establish WAN connection using VPN technology between two distant networks that may be thousands of miles apart, but where each has some way of accessing the internet.
  - ➢ To establish remote access connections that enable remote users to access a private network through a public network like the internet.

➢ VPN's support WAN connection in the same way as they support a remote access connection.

VPN Protocols

- VPN connection must be connected to the internet using point-to-point protocols.

- Both sides must have a networking protocol in common.

- This protocol is usually IP, but can also be IPX, Net BEUI, or Apple talk.

- Both sides must set up a tunnel through their existing PPP connections, through which their data packets will pass.

- The tunnel is formed using a tunneling protocol.

- The three important tunneling protocols used for VPN's are point-to-point tunneling protocol, Layer2 Tunneling Protocol and Internet Protocol Security.

- VPN Client

- VPN connection of both sides must be running compatible VPN software compatible protocols.

- For a remote access VPN solution, the software you install depends on the VPN itself.

- Dedicated VPN solutions also sell client software that you can distribute to users.