Roll no : 03055102713

MVSIT

Ques 1 What is the Internet Protocol (IP)?

The Internet Protocol (IP) is a protocol, or set of rules for routing and addressing packets of data so that they can travel across networks and arrive at the correct destination. Data traversing the Internet is divided into smaller pieces, called packets. IP information is attached to each packet, and this information helps routers to send packets to the right place. Every device or domain that connects to the internet is assigned an IP address, and as packets are directed to the IP address attached to them, data arrives where it is needed.

Once the packets arrive at their destination, they are handled differently depending on which transport protocol is used in combination with IP. The most common transport protocols are TCP and UDP.

Ques 2 Give brief idea of various type of Internet protocol

(a) TCP/ip TCP/IP stands for Transmission Control Protocol/ Internet Protocol. It is a set of conventions or rules and methods that are used to interconnect network devices on the Internet.

The internet protocol suite is commonly known as TCP/IP as the foundational protocols in the suite are Transmission

Control Protocol and Internet Protocol.

It chooses how the information will be traded over the web through end-to-end communications that incorporate how the information ought to be organized into bundles (bundles of data), addressed, sent, and received at the goal.
This communication protocol can also be utilized to interconnect organize devices in a private network such as an intranet or an extranet.

Application/Uses of TCP/IP:-
Simple Mail Transfer Protocol (SMTP): It helps to send email to another email address.
File Transfer Protocol (FTP): It is used for sending large files.
Dynamic Host Configure Protocol (DHCP): It assigns the IP address.

(b) IPv4 IP stands for Internet Protocol and v4 stands for Version Four (IPv4). IP version four addresses are 32-bit integers which will be expressed in decimal notation.
Example- 192.0.2.126 could be an IPv4 address.
IPv4 is responsible for identifying hosts (computers) based on their logical addresses (IPv4 addresses) and routing data among them over the underlying network (Internet). As such

IPv4 provides a way to identify hosts using an IP addressing scheme uniquely. Note, however, that IPv4 uses best-effort delivery. It means that delivery to the desired host is not guaranteed but the protocol will do its best to reach the destination. IPv4 uses 32-bit logical addresses, more commonly known as "IP addresses."

(c) IPv6 IPv6 is the next generation Internet Protocol (IP) standard intended to eventually replace IPv4, the protocol many Internet services still use today. Every computer, mobile phone, and any other device connected to the Internet needs a numerical IP address in order to communicate with other devices. The original IP address scheme, called IPv4, is running out of addresses.

Advantages of IPv6:-

1. Reliability
2. Faster Speeds: IPv6 supports multicast rather than broadcast in IPv4.
3. IPSecurity, which provides confidentiality, and data integrity, is embedded into IPv6.
4. Routing efficiency

Ques 3 What are the security considerations & challenges related to mobile devices and mobile wireless computing?

Mobile computing provides a variety of wireless devices that has the mobility to allow people to connect to the internet. It provides wireless transmission to access data and information from the locations they are stored.

There are mainly three aspects of Mobile computing

(a) -Mobile communication: This aspect specifies the communication issues in ad-hoc, infrastructure networks, communication properties, protocols, data formats and concrete technologies.

(b) Mobile hardware: This aspect specifies the mobile devices or device components that are used in mobile computing.

(c) Mobile software: This aspect specifies all the necessary files and software related to the computer used in mobile computing.

General Security Issues-

There are mainly five fundamental goals of security used in the information system to deal with security issues. They are:

(1) Confidentiality

This is used to prevent unauthorized users from gaining access to any particular user's critical and confidential information.

(2) Integrity

(3) This is used to ensure that any type of unauthorized modification destruction or creation of information cannot be done.

(4) Availability

The availability is used to ensure that authorized users get the required access whenever they need it.

(5) Legitimate

This is used to ensure that only authorized and legitimate users have access to the services.

(6) Accountability

Accountability is used to ensure that the users will be responsible for their security-related activities by arranging the users and their activities in a linked form. We have to achieve these goals according to the security policy used by the service providers.

Wireless Security Issues-

Wireless security issues are considered as the primary security issues of mobile computing. These are related to wireless networks. These issues occur when the hackers intercept the radio signals. Most wireless networks are dependent on other private networks which are managed by others, so after these issues, the users have less control of security procedures. These security issues are;

(1) Denial of Service (DOS) attacks

The denial of services or DOS attacks is one of the most common attacks of all kinds of networks and especially in a wireless network. It prevents users from using network services because the attacker sends a large amount of unnecessary data or connection requests to the communication server. It causes a slow network, and therefore the users cannot get benefitted from using its service.

(2) Traffic Analysis

Traffic analysis is used to identify and monitor communication between users. In this process, the service provider listens the traffic flowing in the wireless channel to access the private information of users affected by the attacker.

(3) Eavesdropping

It specifies that the attacker can log on to the wireless network and access sensitive data if the wireless network was not secure enough. This can also be done if the information is not encrypted.

(4) Session Interception and Messages Modification

It specifies that the attacker can intercept the session and modify the transmitted data in this session. This scenario is called "man in the middle." It inserts the attacker's host between the sender and receiver host.

(5) Spoofing

In this security issue, the attacker impersonates him as an authorized account of another user and tries to access the sensitive data and unauthorized services.

(6) Captured and Retransmitted Messages

In this security issue, the attacker can get some of the network services by getting unauthorized access. After capturing the message, he/she can reply to it with some modifications to the same destination or another.