Unit V

Application Layer: Basic Concept of Application Layer: Domain Name System, World Wide Web, Hyper Text Transfer Protocol, Electronic mail, File Transfer Protocol, Remote login. Introduction to Cryptography: Definition, Goal, Applications, Attacks, Encryption, decryption, public-key and private key cryptography.

Application layer

An application layer is an abstraction layer that specifies the shared communications protocols and interface methods used by hosts in a communications network. An application layer abstraction is specified in both the Internet Protocol Suite (TCP/IP) and the OSI model. Although both models use the same term for their respective highest-level layer, the detailed definitions and purposes are different.

In the Internet protocol suite, the application layer contains the communications protocols and interface methods used in process-to-process communications across an Internet Protocol (IP) computer network. The application layer only standardizes communication and depends upon the underlying transport layer protocols to establish host-to-host data transfer channels and manage the data exchange in a client–server or peer-to-peer networking model.

Domain Name System

The Domain Name System (DNS) is the hierarchical and decentralized naming system used to identify computers, services, and other resources reachable through the internet or other internet protocol networks. The resource records contained in the DNS associate domain names with other forms of information. These are most commonly used to map human-friendly domain names to the numerical IP addresses computers need to locate services and devices using the underlying network protocols, but have been extended over time to perform many other functions as well. The Domain Name System has been an essential component of the functionality of the Internet since 1985.

An often-used analogy to explain the Domain Name System is that it serves as the phone book for the Internet by translating human-friendly computer hostnames into IP addresses. For example, the domain name www.example.com translates to the addresses 93.184.216.34 (IPv4) and 2606:2800:220:1:248:1893:25c8:1946 (IPv6). The DNS can be quickly and transparently updated, allowing a service's location on the network to change without affecting the end users, who continue to use the same hostname. Users take advantage of this when they use meaningful Uniform Resource Locators (URLs) and e-mail addresses without having to know how the computer actually locates the services.An important and ubiquitous function of the DNS is its central role in distributed Internet services such as cloud services and content delivery networks. When a user accesses a distributed Internet service using a URL, the domain name of the URL is translated to the IP address of a server that is proximal to the user. The key functionality of the DNS exploited here is that different users can simultaneously receive different translations for the same domain name, a key point of divergence from a traditional phone-book view of the DNS. This process of using the DNS to assign proximal servers to users is key to providing faster and more reliable responses on the Internet and is widely used by most major Internet services.

World Wide Web

The World Wide Web (WWW), commonly known as the Web, is an information system where documents and other web resources are identified by Uniform Resource Locators (URLs, such as https://example.com/), which may be interlinked by hyperlinks, and are accessible over the Internet. The resources of the Web are transferred via the Hypertext Transfer Protocol (HTTP), may be accessed by users by a software application called a web browser, and are published by a software application called a web server. The World Wide Web is not synonymous with the Internet, which pre-dated the Web in some form by over two decades and upon the technologies of which the Web is built.

English scientist Tim Berners-Lee co-invented the World Wide Web in 1989 along with Robert Cailliau. He wrote the first web browser in 1990 while employed at CERN near Geneva, Switzerland. The browser was released outside CERN to other research institutions starting in January 1991, and then to the general public in August 1991. The Web began to enter everyday use in 1993–1994, when websites for general use started to become available. The World Wide Web has been central to the development of the Information Age and is the primary tool billions of people use to interact on the Internet.

Web resources may be any type of downloaded media, but web pages are hypertext documents formatted in Hypertext Markup Language (HTML).] Special HTML syntax displays embedded hyperlinks with URLs, which permits users to navigate to other web resources. In addition to text, web pages may contain references to images, video, audio, and software components, which are either displayed or internally executed in the user's web browser to render pages or streams of multimedia content.

Multiple web resources with a common theme and usually a common domain name make up a website. Websites are stored in computers that are running a web server, which is a program that responds to requests made over the Internet from web browsers running on a user's computer. Website content can be provided by a publisher or interactively from user-generated content. Websites are provided for a myriad of informative, entertainment, commercial, and governmental reasons.

Hypertext Transfer Protocol

The Hypertext Transfer Protocol (HTTP) is an application layer protocol in the Internet protocol suite model for distributed, collaborative, hypermedia information systems. HTTP is the foundation of data communication for the World Wide Web, where hypertext documents include hyperlinks to other resources that the user can easily access, for example by a mouse click or by tapping the screen in a web browser.

Development of HTTP was initiated by Tim Berners-Lee at CERN in 1989 and summarized in a simple document describing the behavior of a client and a server using the first HTTP protocol version that was named 0.9.

That first version of HTTP protocol soon evolved into a more elaborated version that was the first draft toward a far future version 1.0.

HTTP functions as a request–response protocol in the client–server model. A web browser, for example, may be the client and a process, named web server, running on a computer hosting one or more websites may be the server. The client submits an HTTP request message to the server. The server, which provides resources such as HTML files and other content or performs other functions on behalf of the client, returns a response message to the client. The response contains completion status information about the request and may also contain requested content in its message body.

A web browser is an example of a user agent (UA). Other types of user agent include the indexing software used by search providers (web crawlers), voice browsers, mobile apps, and other software that accesses, consumes, or displays web content.

Electronic Mail

Electronic Mail (e-mail) is one of most widely used services of Internet. This service allows an Internet user to send a message in formatted manner (mail) to the other Internet user in any part of world. Message in mail not only contain text, but it also contains images, audio and videos data. The person who is sending mail is called sender and person who receives mail is called recipient. It is just like postal mail service.

Components of E-Mail System :

The basic components of an email system are : User Agent (UA), Message Transfer Agent (MTA), Mail Box, and Spool file. These are explained as following below.

1. User Agent (UA) :
   The UA is normally a program which is used to send and receive mail. Sometimes, it is called as mail reader. It accepts variety of commands for composing, receiving and replying to messages as well as for manipulation of the mailboxes.
2. Message Transfer Agent (MTA) :
   MTA is actually responsible for transfer of mail from one system to another. To send a mail, a system must have client MTA and system MTA. It transfer mail to mailboxes of recipients if they are connected in the same machine. It delivers mail to peer MTA if destination mailbox is in another machine. The delivery from one MTA to another MTA is done by Simple Mail Transfer Protocol.
3. Mailbox :
   It is a file on local hard drive to collect mails. Delivered mails are present in this file. The user can read it delete it according to his/her requirement. To use e-mail system each user must have a mailbox . Access to mailbox is only to owner of mailbox.
4. Spool file :
   This file contains mails that are to be sent. User agent appends outgoing mails in this file using SMTP. MTA extracts pending mail from spool file for their delivery. E-mail allows one name, an alias, to represent several different e-mail addresses. It is known as mailing list, Whenever user have to sent a message, system checks recipients's name against alias database. If mailing list is present for defined alias, separate messages, one for each entry in the list, must be prepared and handed to MTA. If for defined alias, there is no such mailing list is present, name itself becomes naming address and a single message is delivered to mail transfer entity.

Services provided by E-mail system:

- Composition –
  The composition refer to process that creates messages and answers. For composition any kind of text editor can be used.
- Transfer –
  Transfer means sending procedure of mail i.e. from the sender to recipient.

- Reporting –
  Reporting refers to confirmation for delivery of mail. It help user to check whether their mail is delivered, lost or rejected.
- Displaying –
  It refers to present mail in form that is understand by the user.
- Disposition –
  This step concern with recipient that what will recipient do after receiving mail i.e save mail, delete before reading or delete after reading.

File Transfer Protocol

The File Transfer Protocol (FTP) is a standard communication protocol used for the transfer of computer files from a server to a client on a computer network. FTP is built on a client–server model architecture using separate control and data connections between the client and the server. FTP users may authenticate themselves with a clear-text sign-in protocol, normally in the form of a username and password, but can connect anonymously if the server is configured to allow it. For secure transmission that protects the username and password, and encrypts the content, FTP is often secured with SSL/TLS (FTPS) or replaced with SSH File Transfer Protocol (SFTP). The first FTP client applications were command-line programs developed before operating systems had graphical user interfaces, and are still shipped with most Windows, Unix, and Linux operating systems. Many FTP clients and automation utilities have since been developed for desktops, servers, mobile devices, and hardware, and FTP has been incorporated into productivity applications, such as HTML editors.

Remote Login

Remote Login **is** a process in which user can login into remote site i.e. computer and use services that are available on the remote computer. With the help of remote login a user is able to understand result of transferring result of processing from the remote computer to the local computer.
It is implemented using Telnet.

Procedure of Remote Login

1. When the user types something on local computer, then local operating system accepts character.
2. Local computer does not interpret the characters, it will send them to TELNET client.
3. TELNET client transforms these characters to a universal character set called Network Virtual Terminal (NVT) characters and it will pass them to the local TCP/IP protocol Stack.
4. Commands or text which is in the form of NVT, travel through Internet and it will arrive at the TCP/IP stack at remote computer.
5. Characters are then delivered to operating system and which later on passed to TELNET server.
6. Then TELNET server changes that characters to characters which can be understandable by remote computer.
7. Remote operating system receives character from a pseudo-terminal driver, which is a piece of software that pretends that characters are coming from a terminal.
8. Operating system then passes character to the appropriate application program.

Cryptography

Cryptography is the practice and study of techniques for secure communication in the presence of adversarial behavior.] More generally, cryptography is about constructing and analyzing protocols that prevent third parties or the public from reading private messages; various aspects in information security such as data confidentiality, data integrity, authentication, and non-repudiation are central to modern cryptography. Modern cryptography exists at the intersection of the disciplines of mathematics, computer science, electrical engineering, communication science, and physics. Applications of cryptography include electronic commerce, chip-based payment cards, digital currencies, computer passwords, and military communications.

Cryptography prior to the modern age was effectively synonymous with **encryption,** converting information from a readable state to unintelligible nonsense. The sender of an encrypted message shares the decoding technique only with intended recipients to preclude access from adversaries. The cryptography literature often uses the names Alice ("A") for the sender, Bob ("B") for the intended recipient, and Eve ("eavesdropper") for the adversary.[5] Since the development of rotor cipher machines in World War I and the advent of computers in World War II, cryptography methods have become increasingly complex and its applications more varied.

Cryptography referred almost exclusively to **encryption**, which is the process of converting ordinary information (called **plaintext**) into unintelligible form (called **ciphertext**). **Decryption** is the reverse, in other words, moving from the unintelligible ciphertext back to plaintext.
A *cipher* (or *cypher*) is a pair of algorithms that carry out the encryption and the reversing decryption. The detailed operation of a cipher is controlled both by the algorithm and, in each instance, by a "key". The key is a secret (ideally known only to the communicants), usually a string of characters (ideally short so it can be remembered by the user), which is needed to decrypt the ciphertext.
Historically, ciphers were often used directly for encryption or decryption without additional procedures such as authentication or integrity checks. There are, generally, two kinds of cryptosystems: **symmetric and asymmetric**. In symmetric systems, the only ones known until the 1970s, the same key (the **secret key**) is used to encrypt and decrypt a message. Data manipulation in symmetric systems is faster than asymmetric systems in part because they generally use shorter key lengths. Asymmetric systems use a "**public key**" to encrypt a message and a related "private key" to decrypt it. The use of asymmetric systems enhances the security of communication, largely because the relation between the two keys is very hard to discover. Examples of asymmetric systems include **RSA (Rivest–Shamir–Adleman), and ECC (Elliptic Curve Cryptography)**.