NAME: OGUNWALE PROGRESS OBALOLUWA
DEPARTMENT: COMPUTER SCIENCE
MATRIC NUMBER: RUN/CMP/24/18052
COURSE: CSC 828 - INTERNET TECHNOLOGY
LECTURER: DR. ADEPOJU S.A.

1. The Concept of Synchronous and Asynchronous Communication

1.1 Synchronous Communication

In Synchronous communication data is sent in the form of blocks or frames. This transmission is the full-duplex type, between sender and receiver, synchronization is compulsory. It occurs when people interact in real time, either face-to-face or through digital platforms. Synchronous transmission needs no time gap present between data. It is more efficient and more reliable than asynchronous transmission to transfer a large amount of data.

Both the sender and receiver are synchronized with a common clock signal. This means they operate at the same speed and know exactly when to send and receive data. Data is sent in a continuous stream, with each byte or chunk of data following the previous one without any gaps. It's efficient for sending large amounts of data quickly because there's less overhead (extra bits) needed to start and stop the transmission.

It is like having a live conversation where participants are engaged simultaneously, exchanging immediate responses. This type of communication is common in meetings, phone calls, or live chats where prompt feedback is essential.

Examples:

a. Chat Rooms

b. Telephonic Conversations

c. Video Conferencing

1.2 Asynchronous Communication

In Asynchronous Transmission, data is sent in form of byte or character. This transmission is the half-duplex type transmission. In this transmission start bits and stop bits are added with data. It does not require synchronization. Asynchronous transmission is like sending individual text messages without knowing exactly when the other person will read them.

The sender and receiver do not share a common clock signal. Instead, data is sent one byte or character at a time, with start and stop bits indicating the beginning and end of each byte. Each piece of data is sent independently, with gaps in between, allowing the receiver to process each byte as it arrives. It's flexible and simpler to implement, especially useful for communications where data is sent intermittently.

Example:

a. Emails

b. Forums

c. Letters

2. DOM

The Document Object Model (DOM) is an application programming interface (API) for HTML and XML documents. It defines the logical structure of documents and the way a document is accessed and manipulated. In the DOM specification, the term "document" is used in the broad sense - increasingly, XML is being used as a way of representing many different kinds of information that may be stored in diverse systems, and much of this would traditionally be seen as data rather than as documents. Nevertheless, XML presents this data as documents, and the DOM may be used to manage this data.

With the Document Object Model, programmers can build documents, navigate their structure, and add, modify, or delete elements and content. Anything found in an HTML or XML document can be accessed, changed, deleted, or added using the Document Object Model, with a few exceptions - in particular, the DOM interfaces for the XML internal and external subsets have not yet been specified. The name "Document Object Model" was chosen because it is an "object model" in the traditional object oriented design sense: documents are modeled using objects, and the model encompasses not only the structure of a document, but also the behavior of a document and the objects of which it is composed.

3. Sessions and Cookies

3.1 Sessions

Sessions are a way of storing information about a user on the server-side. Those information will then be used in subsequent requests. By definition, a Web session is a sequence of network HTTP request and response transactions associated with the same user.

Sessions provides the ability to establish variables, such as access rights and localization settings, which will apply to each and every interaction a user has with the web application for the duration of the session.

3.2 Cookies

Cookies provide a way for web applications to store information in the user’s browser. This information can be retrieved every time the user requests a page from the same web server that created the cookies.

Cookies can be either first-party or third-party. First-party cookies are created by the website that the user is visiting, while third-party cookies are created by domains other than the website being visited. Third-party cookies are often used for advertising and tracking purposes.

When a browser request a web page, the server create a cookie and return it to the browser as part of the response. The browser then store that cookie in the user’s computer.

Cookies have a expired date that’s set by the server, when that date come, the cookie will be deleted from the user’s browser. The browser send back that cookie each time it request a web page from that server. Browsers generally accept only 20 cookie from each site, and 300 cookies in total.

4. Malware

Malware, short for malicious software, refers to any intrusive software developed by cybercriminals (often called hackers) to steal data and damage or destroy computers and computer systems. Examples of common malware include viruses, worms, Trojan viruses, spyware, adware, and ransomware.

Malware is developed as harmful software that invades or corrupts your computer network. The goal of malware is to cause havoc and steal information or resources for monetary gain or sheer sabotage intent.

Malware can typically perform the following harmful actions:

Data Ex-filtration

Data ex-filtration is a common objective of malware. During data ex-filtration, once a system is infected with malware, threat actors can steal sensitive information stored on the system, such as emails, passwords, intellectual property, financial information and login credentials. Data ex-filtration can result in monetary or reputational damage to individuals and organizations.

Service Disruption

Malware can disrupt services in several ways. For example, it can lock up computers and make them unusable or hold them hostage for financial gain by performing a ransomware attack. Malware can also target critical infrastructure, such as power grids, healthcare facilities or transportation systems to cause service disruptions.

Data Espionage

A type of malware known as spyware performs data espionage by spying on users. Typically, hackers use key-loggers to record keystrokes, access web cameras and microphones and capture screenshots.

Identity Theft

Malware can be used to steal personal data which can be used to impersonate victims, commit fraud or gain access to additional resources. According to the IBM X-Force Threat Intelligence Index

2024, there was a 71% rise in cyberattacks using stolen identities in 2023 compared to the previous year.

Stealing Resources

Malware can use stolen system resources to send spam emails, operate botnets and run crypto-mining software, also known as cryptojacking.

System Damage

Certain types of malware, such as computer worms, can damage devices by corrupting the system files, deleting data or changing system settings. This damage can lead to an unstable or unusable system.

5. Viruses, Worms, Trojans, Ransomware and Spyware

5.1 Viruses

A virus is the most common type of malware. A virus is a contagious program or code that attaches itself to another piece of software, and then reproduces itself when that software is run. Most often this is spread by sharing software or files between computers.

5.2 Worms

A program that replicates itself and destroys data and files on the computer. Worms work to “eat” the system operating files and data files until the drive is empty. It can self-replicate without a host program and typically spreads without any interaction from the malware authors.

5.3 Trojan

A Trojan horse or Trojan is a type of malware that is often disguised as legitimate software to gain access to a system. Trojans are written with the purpose of discovering your financial information, taking over your computer’s system resources, and in larger systems creating a “denial-of-service attack” which is making a machine or network resource unavailable to those attempting to reach it.

5.4 Ransomware

Ransomware is a type of malicious software that threatens to publish the victim's data or perpetually block access to it unless a ransom is paid. While some simple ransomware may lock the system in a way that is not difficult for a knowledgeable person to reverse, more advanced malware uses a technique called cryptoviral extortion, which encrypts the victim's files, making them inaccessible, and demands a ransom payment to decrypt them.

5.5 Spyware

Spyware is malicious software that secretly monitors a user’s activity, collects personal or device information, and may send it to third parties without consent. It often tracks browsing habits and can include adware that delivers unwanted ads.