REDEEMER'S UNIVERSITY, EDE

COLLEGE OF POSTGRADUATE STUDIES

COURSE CODE: CIT828

COURSE TITLE: Internet Technology

ASSIGNMENTS:

Explain the concept of Synchronous and Asynchronous Communication

Explain DOM

Sessions and cookies

What is Malware

Differentiate between Viruses, worms, Trojans, Ransomware and Spyware

SUBMITTED TO

Dr. S. A. Adepoju

SUBMITTED BY:

PETER Agnes Aderonke

July 22, 2025

1. **Synchronous and Asynchronous Communication**

   Synchronous communication can be defined as real-time, bidirectional data exchange during which both parties are present and actively participating at the same time. Examples include video conferencing, live chat, and phone calls. This model provides immediate feedback while requiring temporal alignment. In contrast, asynchronous communication does not require participants to be present at the same time. Email, forums and messaging apps are all examples of applications that allow users to answer whenever they want. This model is scalable and suitable for distributed systems with different availability and time zones. In web development, synchronous communication can halt code execution until a task is completed (for example, synchronous JavaScript requests), whereas asynchronous communication allows for non-blocking operations, which are commonly implemented in modern programming using AJAX, Promises, or async/await constructs.

2. **Document Object Model (DOM).**

   The Document Object Model (DOM) provides a programming interface for web content. It depicts an HTML or XML document's structure as an object tree, allowing programs to dynamically access, alter, delete, or add elements and content. To create dynamic online experiences, JavaScript interacts with each element (e.g., , <p>) as a node in the tree, using the DOM API.

   The DOM is language-neutral, but is most commonly controlled with JavaScript. Modern browsers support DOM Levels 3 and higher, which enable extensive manipulation features such as event handling, style, and traversal methods.

3. **Sessions and Cookies**

Cookies are little bits of information that the server stores on the client's browser and are used to remember user information across requests, like user preferences or authentication tokens. They are part of every HTTP request, which makes them appropriate for client-side state management. On the other hand, server-side storage methods known as sessions record user interactions over a number of requests. often, the server sends the client a Session ID, which is often kept in a cookie, to start a session. In order for the server to obtain related data, the client must include the Session ID with any further requests. Sessions are typically more secure because they are handled and stored on the server, although cookies can be altered or expire by the client.

4. **Malware**

Software created with the intention of causing disruption, harm, or gaining illegal access to computer systems or data is referred to as malware, or malicious software. Malware comes in many forms, including Trojan horses, worms, viruses, ransomware, and spyware. It can lead to financial and reputational losses, compromise system integrity, or steal confidential data.

Phishing, malicious attachments, software flaws, and social engineering are some of the ways that modern malware spreads and is frequently polymorphic. To fight malware, cybersecurity frameworks use detection systems like endpoint detection and response (EDR) technologies, behavior-based threat analysis, and antivirus software.

5. Differences Between Viruses, Worms, Trojans, Ransomware, and Spyware

Type	Description	Propagation Method	Impact
Virus	Attaches itself to files or programs and spreads when the host is executed.	File-sharing, email attachments	Corrupts or deletes files, degrades system performance
Worm	Self-replicating; spreads across networks without user action.	Exploits network vulnerabilities	Bandwidth consumption, system crashes
Trojan	Disguised as legitimate software to trick users into executing it.	Social engineering, downloads	Opens backdoors, steals data
Ransomware	Encrypts user data and demands payment for decryption keys.	Email phishing, RDP exploits	Data loss, financial damage
Spyware	Secretly monitors user activity and collects sensitive data.	Bundled with freeware, ads	Identity theft, privacy invasion

References

Alazab, M., & Awajan, A. (2021). Cybersecurity and malware detection using AI and ML. *Journal of Cyber Security Technology, 5*(2), 91–104

Jadhav, S., & Patil, V. (2022). Web application state management techniques: A comparative analysis. *International Journal of Web & Semantic Technology (IJWesT), 13*(1), 1–10

Kumar, P., & Singh, A. (2021). Asynchronous communication in modern web applications: A comparative study. *International Journal of Computer Applications, 183*(20), 17–21

Mozilla Developer Network (MDN). (2023). *Introduction to the DOM*

Singh, G., & Arora, A. (2020). A comprehensive taxonomy of malware threats in modern computing systems. *Computers & Security, 95*, 101876