Module-I: Introduction to Cyber security

Defining Cyberspace and Overview of Computer and Web-technology, Architecture of cyberspace, Communication and web technology, Internet, World wide web, Advent of internet, Internet infrastructure for data transfer and governance, Internet society, Regulation of cyberspace, Concept of cyber security, Issues and challenges of cyber security.

Defining Cyberspace

- The term Cyberspace was first coined by William Gibson in the year 1984.
- Cyberspace is the environment in which communication over computer networks occurs.
- Cyberspace is the virtual and dynamic space created by the machine clones. Cyberspace mainly refers to the computer which is a virtual network and is a medium electronically designed to help online communications to occur.
- The primary purpose of creating cyberspace is to share information and communicate across the globe.
- Cyberspace is that space in which users share information, interact with each other; engage in discussions or social media platforms, and many other activities.
- The whole Cyberspace is composed of large computer networks which have many sub-networks. These follow the TCP or IP protocol.

Overview of Computer and Web-technology

Computer and web technology are integral parts of our modern world, shaping how we communicate, work, learn, and entertain ourselves.

Computer Technology:

1. **Hardware:** Computers consist of physical components like the central processing unit (CPU), memory (RAM), storage devices (HDD/SSD), input/output devices (keyboard, mouse, monitor), and more. These components work together to process and store data.
2. **Software:** Software includes the operating system (e.g., Windows, macOS, Linux) and various applications (e.g., Microsoft Office, web browsers, video games) that run on a computer. Operating systems manage hardware resources and provide a user interface.

3. **Networking:** Computers can connect to each other and the internet via wired (e.g., Ethernet) or wireless (e.g., Wi-Fi) networks. Networking enables data sharing, communication, and remote access.
4. **Security:** Computer security is crucial to protect data and systems from threats like viruses, malware, and hackers. Antivirus software, firewalls, and encryption are common security measures.
5. **Processing Power:** Moore's Law predicts that the processing power of computers doubles approximately every two years. This constant improvement drives innovations in various fields, including artificial intelligence, scientific research, and data analysis.

Web Technology:

1. **World Wide Web (WWW):** The World Wide Web, commonly referred to as the web, is a global system of interconnected documents and resources linked through hyperlinks. It is accessed via web browsers.
2. **Web Browsers:** Web browsers like Google Chrome, Mozilla Firefox, and Microsoft Edge allow users to access and interact with web content.
3. **Web Development:** Web development involves creating and maintaining websites and web applications.
4. **Web Servers:** Web servers store and deliver web content to users' browsers upon request. Popular web server software includes Apache, Microsoft IIS.
5. **Web Security:** Ensuring web security is critical to protect data and user privacy. Measures include SSL/TLS encryption, secure authentication, and regular security audits.
6. **Web Standards:** Organizations like the World Wide Web Consortium (W3C) establish web standards to ensure compatibility and accessibility across different devices and browsers.

Architecture of cyberspace

There isn't a single, specific architecture for cyberspace, as it encompasses a wide range of technologies, protocols, and platforms. Some key components and concepts related to the architecture of cyberspace are:

1. **Network Infrastructure:** At the core of cyberspace is the global network infrastructure, often referred to as the Internet. This infrastructure comprises a vast array of

interconnected physical and virtual components, including routers, switches, data centers, and undersea cables. The Internet's architecture is based on the Internet Protocol (IP), which allows data packets to be routed across the network.

2. **Protocols:** Various communication protocols define how data is transmitted and received in cyberspace. The Transmission Control Protocol (TCP) and Internet Protocol (IP) are fundamental to the functioning of the Internet. Other protocols like HTTP (Hypertext Transfer Protocol), SMTP (Simple Mail Transfer Protocol), and FTP (File Transfer Protocol) govern specific types of data exchange.
3. **Domain Name System (DNS):** DNS is a crucial component of cyberspace that translates human-readable domain names (e.g., www.example.com) into IP addresses. This system enables users to access websites and resources by name rather than needing to remember numeric IP addresses.
4. **Data Centers:** Data centers house the servers and storage infrastructure that store and deliver digital content and services. They play a pivotal role in hosting websites, applications, and cloud services.
5. **Cybersecurity:** The architecture of cyberspace includes various security measures to protect data, networks, and users. Firewalls, encryption, intrusion detection systems, and antivirus software are examples of cybersecurity components.
6. **Web and Application Servers:** These servers host websites, web applications, and other online services. They respond to user requests, retrieve data from databases, and deliver content to users' devices.
7. **User Devices:** These are the various devices through which users access cyberspace, including computers, smartphones, tablets, and IoT devices. Each device has its own hardware and software components that enable connectivity and interaction with cyberspace.
8. **Cloud Computing:** Cloud services and platforms are an integral part of cyberspace architecture. Cloud providers offer scalable computing resources, storage, and services, allowing organizations to leverage the cloud for various purposes.
9. **Social Media and Online Communities:** Cyberspace also includes virtual communities and social media platforms that enable users to connect, share information, and collaborate online. These platforms have their own architectures and algorithms for content delivery and interaction.

10. **Internet of Things (IoT):** IoT devices are connected to cyberspace, enabling them to collect and exchange data with other devices and systems. They play a role in creating the "smart" aspect of cyberspace, connecting physical objects to the digital realm.
11. **Regulations and Governance:** Various laws and regulations govern cyberspace to ensure security, privacy, and fair use. Organizations like ICANN (Internet Corporation for Assigned Names and Numbers) oversee domain name management, while governments have jurisdiction over aspects like data protection and cybersecurity.

Cyberspace is a dynamic and evolving environment, with new technologies and architectures continually emerging. Its architecture is shaped by the needs of users, businesses, governments, and the broader digital ecosystem. As such, it remains a subject of ongoing development, discussion, and adaptation.

Communication and web technology

Communication and web technology are integral components of the modern digital landscape. They encompass a wide range of technologies and tools that facilitate communication and the dissemination of information over the internet. Some key aspects of communication and web technology are:

1. **Internet:** The internet is the foundation of web technology. It is a global network of interconnected computers and servers that allows for the transfer of data and information across the world.
2. **Web Browsers:** Web browsers like Chrome, Firefox, Safari, and Edge are software applications that enable users to access and interact with websites and web-based applications.
3. **Websites:** Websites are collections of web pages that are hosted on web servers and can be accessed through a web browser. They are created using various web technologies such as HTML, CSS, and JavaScript.
4. **Web Development:** Web development involves designing, creating, and maintaining websites. Web developers use various programming languages and frameworks to build web applications and sites.
5. **Web Standards and Protocols:** Various standards and protocols govern web technology, including HTTP/HTTPS (for data transfer), HTML5, CSS3, and more.

6. **Mobile Web:** Mobile web technology focuses on optimizing websites and applications for mobile devices, ensuring a seamless user experience on smartphones and tablets.

Internet

- The word Internet is derived from the word internetwork, or the connecting together two or more computer networks.
- The Internet started in the 1960s as a way for government researchers to share information.
- Computers in the '60s were large and immobile and in order to make use of information stored in any one computer, one had to either travel to the site of the computer or have magnetic computer tapes sent through the conventional postal system.
- January 1, 1983 is considered the official birthday of the Internet. Prior to this, the various computer networks did not have a standard way to communicate with each other.
- A new communications protocol was established called Transfer Control Protocol/Internetwork Protocol (TCP/IP). This allowed different kinds of computers on different networks to "talk" to each other.
- **Transmission Control Protocol/Internet Protocol (TCP/IP)**
  - TCP/IP is a suite of communication protocols used to interconnect network devices on the Internet.
  - TCP establishes the connections between sending and receiving computers, and makes sure that packets sent by one computer are received in the same sequence by the other, without any packets missing.
  - IP provides the Internet’s addressing scheme and is responsible for the actual delivery of the packets.
  - TCP/IP is divided into four separate layers, with each layer handling a different aspect of the communication problem.

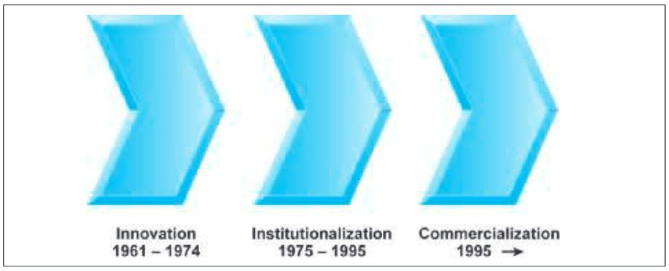
World Wide Web (WWW)

- The World Wide Web was invented by a British scientist, Tim Berners-Lee in 1989.
- World Wide Web, which is also known as a Web, is a collection of websites or web pages stored in web servers and connected to local computers through the internet.

- These websites contain text pages, digital images, audios, videos, etc. Users can access the content of these sites from any part of the world over the internet using their devices such as computers, laptops, cell phones, etc.
- The WWW, along with the internet, enables the retrieval and display of text and media to your device.
- The building blocks of the Web are web pages which are formatted in HTML and connected by links called "hypertext" or hyperlinks and accessed by HTTP.

Advent of internet

- The Internet started off with research into what was then known as packet switching as early as the 1960s.
- ARPANET is considered the first known group of interconnected computers aka the internet. This system was used to transfer confidential data between the Military.
- This data-sharing technology was then opened to educational institutes in the United States to allow them to access to government's supercomputer, first at 56 kbit/s, then at 1.5 Mbit/s, and then at 45 Mbit/s.
- Internet service providers began to arise in the late 1980s and the internet was fully commercialized in the US by 1995.
- The history of the Internet can be segmented into three phases
    1. Innovation Phase
    2. Institutionalization Phase
    3. Commercialization Phase



Innovation Phase (1961 to 1974)

- The fundamental building blocks of the Internet—packet-switching hardware, a communications protocol called TCP/ IP, and client/server computing were conceptualized and then implemented in actual hardware and software.

Institutionalization Phase (1975 to 1995)

- large institutions such as the U.S. Department of Defense (DoD) and the National Science Foundation (NSF) provided funding and legitimization for the fledging Internet.

Commercialization Phase (1995 to the present)

- The U.S. government encouraged private corporations to take over and expand the Internet backbone as well as local service beyond military installations and college campuses to the rest of the population around the world.

Internet infrastructure for data transfer and governance

- Internet infrastructure for data transfer and governance encompasses the physical and virtual systems, protocols, and regulations that enable the secure, efficient, and reliable exchange of data across the global network.
- This infrastructure plays a critical role in ensuring data privacy, security, and compliance with regulations.
- Here are key components and considerations for internet infrastructure related to data transfer and governance:

1. **Network Infrastructure**
   - Backbone Networks: High-speed, long-distance networks that form the core of the internet, connecting major data centers and internet exchange points (IXPs).
   - Last-Mile Connectivity: The connection from service providers to end-users, including wired (e.g., fiber-optic, DSL) and wireless (e.g., 5G, Wi-Fi) technologies.
   - Data Centers: Facilities that house servers and storage devices, providing the infrastructure for web hosting, cloud computing, and data storage.
2. **Protocols and Standards**
   - Internet Protocol (IP): The foundation of internet communication, ensuring data packets can be routed across networks.
   - Transport Layer Security (TLS): Encryption protocol for securing data in transit.
   - Hypertext Transfer Protocol (HTTP) and HTTPS: Protocols for web data transfer, with HTTPS adding a security layer.
   - DNSSEC: Enhances the Domain Name System (DNS) by adding a layer of security through digital signatures.

3. **Data Centers and Cloud Services**
   - Major providers like Amazon Web Services (AWS), Microsoft Azure, and Google Cloud offer robust infrastructure and tools for data storage and processing.
4. **Data Governance and Regulation**
   - Data Privacy Regulations: Compliance with laws like GDPR (in Europe), CCPA (in California), and HIPAA (for healthcare data).
   - Data Retention Policies: Guidelines for storing and managing data for specific periods.
   - Data Access Controls: Systems to restrict and monitor who can access and modify data.
   - Data Encryption: Ensuring data at rest and in transit is properly encrypted to protect against unauthorized access.
5. **Cybersecurity**
   - Robust security measures, including firewalls, intrusion detection systems, and regular security audits, are essential to protect data during transfer.
6. **Internet Governance Bodies**
   - Organizations like ICANN (Internet Corporation for Assigned Names and Numbers) oversee domain name system management and policy.
   - Multistakeholder governance models involve various stakeholders, including governments, businesses, and civil society, in shaping internet governance.
7. **Content Delivery Networks (CDNs)**
   - CDNs like Akamai and Cloudflare optimize data delivery by caching content at various locations worldwide, reducing latency.
8. **Quality of Service (QoS)**
   - Ensuring data transfer meets performance requirements, especially for applications like video conferencing and online gaming.
9. **International Collaboration**
   - Cooperation among nations is essential to establish international norms and agreements related to data transfer and governance.
10. **Data Transfer Agreements**
    - Agreements like Privacy Shield and Standard Contractual Clauses facilitate the lawful transfer of data across borders.

Internet society

- Internet Society (ISOC) A professional membership society that promotes the use and future development of the Internet. It has individual and organization members all over the world and is governed by an elected board of trustees. ISOC coordinates various groups responsible for Internet infrastructure.
- These include
    1. The Internet Engineering Task Force (*IETF*),
    2. The Internet Architecture Board (*IAB*), and
    3. The Internet Engineering Steering Group (*IESG*).
- The IETF develops technical standards for the Internet.
- The IAB has overall responsibility for the architecture and adjudicates on disputes about standards.
- The IESG, along with the IAB, reviews standards proposed by the IETF

Regulation of cyberspace

- Cyberspace spans worldwide, but it has no formal framework. The lack of formal framework makes cyberspace nobody's domain
- No single individual, entity, or government owns or controls cyberspace.
- Regulation in cyberspace is an emerging challenge
- The default in cyberspace is anonymity. Anonymity encourages and enhances the exercise of freedom. A child too shy to express himself in physical space can feign to be somebody else in virtual space, and express himself freely.
- Crimes of global repercussion are also committed with the use of the internet. Trafficking of persons, child pornography, kidnapping for ransom, and terrorism are perpetrated with the use of cyberspace. Freedom thus in cyberspace should not be exercised without the concomitant responsibility of its users.
- Practical Problems In Extending The Traditional Laws To Cyberspace
    1. Multiple Jurisdictions-Because of anonymity of the Internet user, absence of geographical boundaries in the cyberspace, and the cross border effect of Internet transactions, all legal systems face legal uncertainty.

2. Problem of Policing-The lack of technical knowledge, non-co-operation among different police organization etc., make the problem too difficult to be solved.
3. Expensive Process-Training of law enforcement officers to solve the issue of cybercrime is very expensive.
4. Obtaining Digital Evidence- Another instance where the policing of cybercrime becomes difficult is with regard to obtaining the digital evidence.

Concept of cyber security

- cybersecurity is the practice of protecting computer systems, networks, and data from theft, damage, or unauthorized access.
- It encompasses a wide range of technologies, processes, and practices designed to safeguard digital information and ensure the confidentiality, integrity, and availability of data.

1. **Confidentiality**: This principle focuses on ensuring that sensitive information is only accessible to authorized individuals or systems. It involves encryption, access controls, and data classification to prevent unauthorized access or disclosure.
2. **Integrity**: Integrity in cybersecurity means that data and systems are accurate and trustworthy. Any unauthorized modification or tampering with data or systems should be detected and prevented. Techniques like checksums and digital signatures are used to maintain data integrity.
3. **3. Availability**: Availability ensures that systems and data are accessible when needed. Cyberattacks can disrupt services or make them unavailable, so cybersecurity measures aim to prevent or mitigate such disruptions through redundancy, load balancing, and disaster recovery planning.
4. **Authentication**: Authentication is the process of verifying the identity of users, devices, or systems trying to access resources. This can be achieved through passwords, biometrics, two-factor authentication (2FA), and multi-factor authentication (MFA).

Cyber Attacks

- A cyber-attack is an exploitation of computer systems and networks. It uses malicious code to alter computer code, logic or data and lead to cybercrimes, such as information and identity theft.

- Cyber-attacks can be classified into the following categories:
  1. Web-based attacks
  2. System-based attacks

Web-based attacks

- These are the attacks which occur on a website or web applications. Some of the important web-based attacks are as follows-

I. Injection attacks :It is the attack in which some data will be injected into a web application to manipulate the application and fetch the required information.

II. Session Hijacking :It is a security attack on a user session over a protected network. Web applications create cookies to store the state and user sessions. By stealing the cookies, an attacker can have access to all of the user data.

III. Phishing: Phishing is a type of attack which attempts to steal sensitive information like user login credentials and credit card number. It occurs when an attacker is masquerading as a trustworthy entity in electronic communication.

IV. Denial of Service:It is an attack which meant to make a server or network resource unavailable to the users. It accomplishes this by flooding the target with traffic or sending it information that triggers a crash.

System-based attacks

- These are the attacks which are intended to compromise a computer or a computer network. Some of the important system-based attacks are as follows-

I. **Virus :**It is a type of malicious software program that spread throughout the computer files without the knowledge of a user. It is a self-replicating malicious computer program that replicates by inserting copies of itself into other computer programs when executed. It can also execute instructions that cause harm to the system.

II. **Worm :**It is a type of malware whose primary function is to replicate itself to spread to uninfected computers. It works same as the computer virus. Worms often originate from email attachments that appear to be from trusted senders.

III. **Trojan horse : i**t is a malicious program that occurs unexpected changes to computer setting and unusual activity, even when the computer should be idle. It misleads the user of its true intent. It appears to be a normal application but when opened/executed some malicious code will run in the background.

Cyber Threat

- A Cyber threat is any malicious act that attempts to gain access to a computer network without authorization or permission from the owners.
- It refers to the wide range of malicious activities that can damage or disrupt a computer system, a network or the information it contain.

Cyber Threat	Cyber Attack
A Threat by definition is a condition / circumstance which can cause damage to the system/asset.	An Attack by definition is an intended action to cause damage to system/asset.
Threats can be intentional like human negligence or unintentional like natural disasters.	The attack is a deliberate action. An attacker has a motive and plan the attack accordingly.
A Threat may or may not malicious.	An Attack is always malicious.
Chance to damage or information alteration varies from low to very high.	The chance to damage or information alternation is very high.

Issues and challenges of cyber security

- Cybersecurity faces numerous issues and challenges due to the ever-evolving nature of technology and the increasing sophistication of cyber threats.
- Some of the key issues and challenges in cybersecurity include:
  1. **Cyber Attacks:** The constant threat of cyberattacks from various actors, including hackers, cybercriminals, nation-states, and hacktivists, is a significant challenge. These attacks can take various forms, such as malware, ransomware, phishing, and distributed denial of service (DDoS) attacks.
  2. **Data Breaches:** Data breaches can have severe consequences for organizations and individuals. The theft or exposure of sensitive data, such as personal information, financial records, or intellectual property, can lead to financial losses, reputational damage, and legal liabilities.
  3. **Security Vulnerabilities:** Software and hardware vulnerabilities are exploited by attackers to gain unauthorized access or control over systems. Identifying and patching these vulnerabilities in a timely manner is a constant challenge.

4. **Insider Threats:** Insider threats, where individuals within an organization misuse their access and privileges, can be particularly challenging to detect and prevent. This includes employees, contractors, or partners who intentionally or unintentionally compromise security.
5. **Lack of Cybersecurity Awareness:** Many individuals and employees lack awareness of cybersecurity best practices, making them susceptible to social engineering attacks and other cyber threats.
6. **Resource Constraints:** Smaller organizations and even some larger ones may lack the resources and expertise needed to implement robust cybersecurity measures. This can leave them vulnerable to attacks.
7. **Ransomware:** Ransomware attacks have surged in recent years, with cybercriminals encrypting data and demanding a ransom for decryption keys. These attacks can disrupt critical operations and result in significant financial losses.