CYBER SECURITY

MODULE 01: Introduction to Cyber Security

➢ Introduction to Cyber Security:

Cybersecurity is a field dedicated to protecting computer systems, networks, programs, and data from digital attacks, damage, theft, and unauthorized access. As our world becomes increasingly digitized, the importance of cybersecurity has grown exponentially. The interconnected nature of modern technology exposes individuals, organizations, and governments to various cyber threats, making robust cybersecurity measures crucial for safeguarding sensitive information and maintaining the integrity of digital systems.

➢ Meaning of Cyber Space:

Cyberspace refers to the virtual computer world, and more specifically, an electronic medium that is used to facilitate online communication. Cyberspace typically involves a large computer network made up of many worldwide computer subnetworks that employ TCP (Transmission Control Protocol)/IP protocol to aid in communication and data exchange activities.

➢ Concepts of Cyber Space:

Here are key aspects of defining cyberspace:

1. Virtual Environment

Cyberspace is not a tangible place like a physical location but a virtual environment. It is a space where digital data and information exist, flow, and interact

2. Networked Systems

It is created by the interconnection of computer systems, servers, routers, and other network devices. These systems communicate with each other through data transmission protocols, such as the Internet's TCP/IP.

3. Information Exchange

Cyberspace is primarily used for the exchange of information, including text, images, videos, and other digital content. It enables global communication and data sharing.

4. Worldwide Scope

Cyberspace is not limited by geographical boundaries. It is a global domain where individuals, organizations, and governments can connect and interact regardless of their physical locations.

5. Digital Transactions

Online activities like e-commerce, social media, email and web browsing all take place within cyberspace. It is the platform for various digital services and transactions.

Nikitha S
Assistant Professor of Commerce
Basaveshwara College

6. Security Challenges

Cyberspace is vulnerable to various cyber threats and security concerns, including hacking, malware, data breaches, and cyberattacks. As a result, cybersecurity is essential to protect the integrity and privacy of digital information.

7. Legal and Ethical Considerations

Cyberspace raises legal and ethical questions related to digital privacy, intellectual property, online behavior, and cybercrime. Laws and regulations are continually evolving to address these issues.

8. Evolution and Change

Cyberspace is dynamic and constantly evolving as technology advances. New technologies and applications continually reshape the digital landscape, creating new opportunities and challenges.

9. Role in Society

Cyberspace plays a crucial role in modern society, impacting how people communicate, conduct business, access information, entertain themselves, and more. It has transformed various aspects of our daily lives.

10. Digital Culture

Cyberspace has given rise to a unique digital culture, including online communities, virtual worlds, and social norms specific to the online environment.

➢ Overview of Computer:

➢ Definition:

"A device used for computing, specifically, an electronic machine which, by means of stored instructions and information, performs rapid, often complex calculations or compiles, correlates and selects data". **Webster's Dictionary**

➢ Features/Characteristics of Computer:

Today the computer plays a major role in the modern society and its development. The characteristics that make a computer possible to play such vital role are:

(i) High Speed: Since electrical pulses cause all the operations of the computer, the computers can perform large number of operations in just one second. The processing speed of a computer is generally measured in Nano seconds. Since the computers are electronic device and work with the electrical pulses which travel at incredible speed and hence their internal speed is also virtually instantaneous. The speed of the processing varies with the computer hardware.

(ii) Accuracy: The accuracy of the computers is consistently very high. Computers do not make mistakes. Errors causes in computing are generally due to negligence, such as inaccurate data, improper procedures, poor designs etc.

(iii) Storage Capacity: Computers have a very large storage capacity. The computers can store large amount of data and information, which is expressed in terms of kilobytes, megabytes and gigabytes in memory. Moreover, the storage capacity of the computers can be increased by using secondary storage devices such as magnetic disk. The information stored in the secondary storage devices can be retrieved quickly with the help of main memory (RAM).

(iv) Reliability: The computers give very accurate results with predetermined values. They correct and modify the parameters automatically and give suitable signals. They give formatted results with high degree of precision.

(v) Versatility: Computers are very versatile machines with manual and automatic controls. They are capable of solving any problem and can be applied in all sorts of business and other activities.

(vi) Automation: The special feature of computer is automation i.e. the computer executes a program continuously without any human intervention until completion. The central processing unit of the computer makes it processing unit of the computer makes it possible.

➢ Advantages of using Computer:

Benefits from using computers are possible because computers have the advantages of speed, reliability, consistency, storage and communications.

1. Speed: When data, instructions, and information flow along electronic circuits in a computer, they travel at incredibly fast speeds. Many computers process billions or trillions of operations in a single second. Processing involves computing (e.g. adding, subtracting), sorting (e.g., alphabetizing), organizing, displaying images, recording audio, playing music and showing a movie or video.

2. Reliability: The electronic components in modern computers are dependable and reliable because they rarely break or fail.

3. Consistency: Given the same input and processes, a computer will produce the same results consistently. A computing phrase known as garbage in, garbage out-points out that the accuracy of a computer's output depends on the accuracy of the input.

4. Storage: A computer can transfer data quickly from storage to memory, process it and then store it again for future use. Many computers store enormous amounts of data and make this data available for processing anytime it is needed.

5. Communications: Most computers today can communicate with other computers often wirelessly. Computers with this capability can share any of the four information processing cycle operations - input, process, output and storage - with another computer or a user.

Limitations of Computer:

The computer can outperform human beings in speed, memory and accuracy but still the computer has limitations. There are following limitations of a computer.

(i) Programmed by human: Though computer is programmed to work efficiently, fast and accurately but it is programmed by human beings to do so. Without a program, computer is nothing. A program is a set of instructions. Computer only follows these instructions. If the instructions are not accurate the working of computer will not accurate.

(ii) Thinking: The computer cannot think itself. The concept of artificial intelligence shows that the computer can think. But still this concept is dependent on set of instructions provided by the human beings.

(iii) Self Care: A Computer cannot care itself like a human. A computer is dependent still to human beings for this purpose.

(iv) Retrieval of memory: A computer can retrieve data very fast but this technique is linear. A human being's mind does not follow this rule. A human mind can think randomly which a computer machine cannot.

(v) Feelings: One of the main limits in the computer is of feeling. A computer cannot feel about some like a human. A computer cannot meet human in respect of relations. Human can feel, think and caring but a computer machine itself cannot. A computer cannot take place of human because computer is always dependent of human.

Web-technology:

Web technology refers to the broad range of tools, languages, protocols, and practices used in the development and operation of websites and web applications. It encompasses the technologies and methods that enable the functioning of the World Wide Web.

Web technology includes various components and concepts, such as:

1. **Web Development Languages and Technologies**

a) **HTML (Hypertext Markup Language):** The standard markup language used to structure and format content on web pages.

b) **CSS (Cascading Style Sheets):** A stylesheet language used for defining the presentation and layout of web pages, including fonts, colors, and positioning.

c) **JavaScript:** A scripting language that enables interactivity and dynamic behavior on web pages.

d) **Backend Languages**: Such as PHP, Python, Ruby, Java, and Node.js, used for server-side scripting to process data and manage server operations.

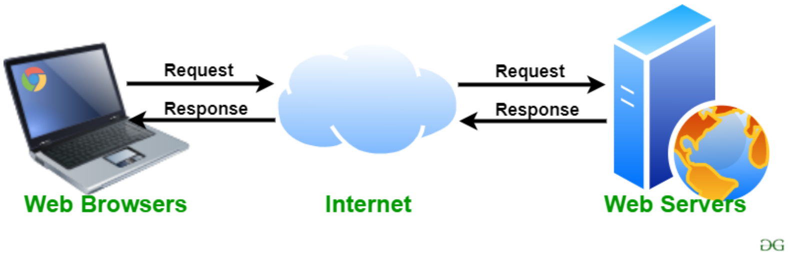
e) **Databases:** Systems like MySQL, PostgreSQL, MongoDB, and SQL Server for data storage and retrieval.

f) **Web Frameworks:** Tools and libraries that simplify web development, such as Ruby on Rails, Django, and Angular.

2. Web Servers and Protocols

a) **HTTP (Hypertext Transfer Protocol):** The foundation of data communication on the web, specifying how messages are formatted and transmitted between the client (browser) and server.

b) **Web Servers**: Software or hardware that hosts websites and serves web content to users, including Apache, Nginx, and Microsoft Internet Information Services (IIS).



3. Web Designs and User Experience (UX)

a) Responsive Design: Designing websites to adapt and function well on various devices and screen sizes.

b) User Interface (UI) Design: Focusing on the layout, visual elements, and interaction design to enhance the user experience.

c) User Experience (UX) Design: Concentrating on creating an intuitive and satisfying experience for website visitors.

4. Content Management Systems (CMS)

Platforms like WordPress, Joomla, and Drupal that facilitate the creation and management of web content.

5. Web Hosting

Web hosting is an online service that allows you to publish your website files onto the internet. So, anyone who has access to the internet has access to your website.

6. Web Security

Techniques and practices for safeguarding websites and web applications from security threats, vulnerabilities, and attacks.

7. **Web Services and APIs (Application Programming Interface)**

   Mechanisms for allowing different software systems to communicate and share data over the web.

8. **Web Standards and Accessibility**

   Adherence to industry standards (eg.W3C standards) and ensuring web content is accessible to people with disabilities.

➢ Classification of Web-Technology

1. World Wide Web (WWW)

The World Wide Web can further be classified into several different technologies They are web browsers, Hyper Text Markup Language (HTML), and Hypertext Transfer Protocol (HTTP).

2. Web Browser

This application software helps explore the World Wide Web (WWW). It provides the user interface between the client and the server. The web browser also requests the server for web documents and services.

3. Web Server:

It is a program that acts upon the network request of the user and serves them with the files that help open the web page. The exchange of files takes place with the help of the Hypertext Transfer Protocol (HTTP).

4. Web Pages:

A web page is the digital document's front-end linked to the World Wide Web. It can be viewed by anyone having an internet connected web browser.

5. Web Development

Web development is everything about building and maintaining websites. It contains web services, including web programming, web publishing, web design, and database management.

➢ Architecture of Cyberspace

Cyberspace architecture can be easily related to a physical parallel. It is like the museum in real life and a model in cyberspace. But buildings in cyberspace are constructed from programming language and not bricks and mortar. Social networking sites such as Facebook, Twitter, and Instagram are examples of cyberspace where people can connect and communicate with each other, regardless of their physical location.

Here's an overview of the architecture of cyberspace:

1. Physical Infrastructure

At the foundational level, the architecture of cyberspace relies on a physical infrastructure composed of network cables, data centers, and various network devices. This infrastructure supports the transmission of data across the globe.

2. Internet Backbone

The internet backbone consists of a vast network of high-capacity data transmission lines and fiber optic cables. It serves as the core of the internet, providing the necessary bandwidth for global data transmission.

3. Protocols and Standards

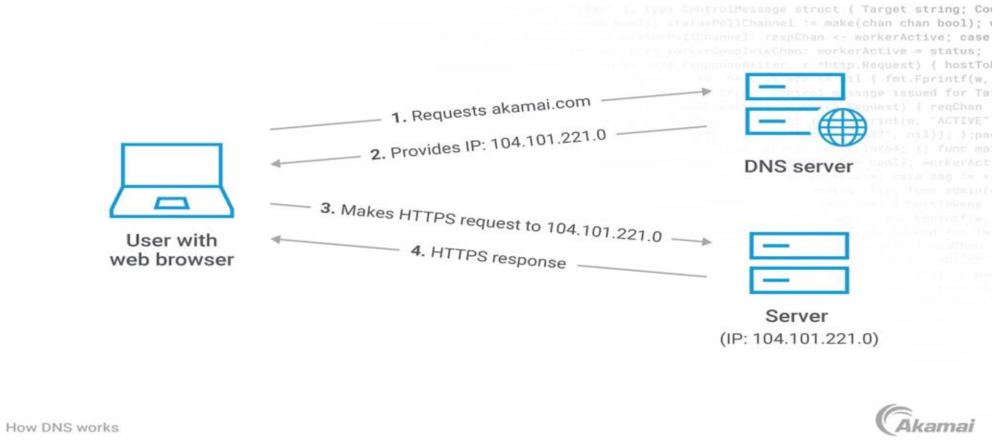
Various protocols and standards govern data transmission and communication on the internet, including:

a) TCP/IP (Transmission Control Protocol/Internet Protocol): The fundamental protocol suite responsible for data transmission across the internet.

b) HTTP/HTTPS (Hypertext Transfer Protocol/Secure): Protocols used for transmitting web content, crucial for websites and web applications.

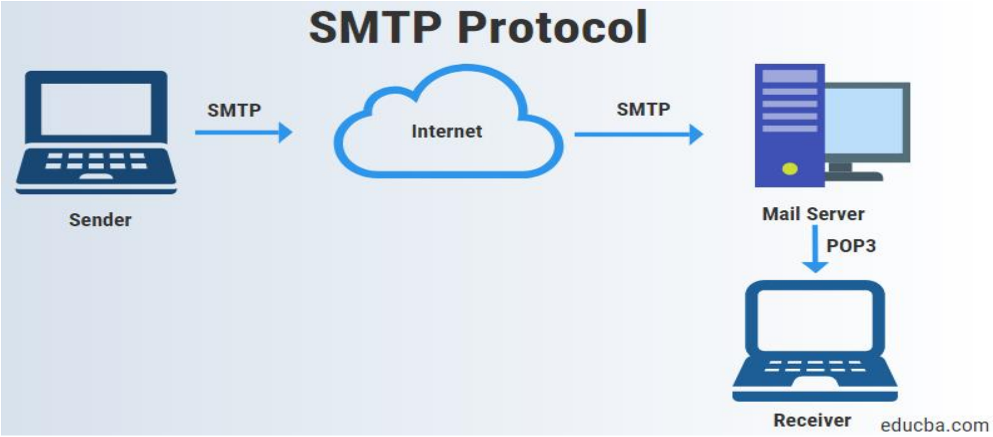
c) FTP (File Transfer Protocol): A protocol for transferring files over the internet.

d) DNS (Domain Name System): A system for translating human readable domain names into IP addresses to locate web servers.
Examples: WWW.amazon.com IP Address 192.02.44.01



How DNS works

e) SMTP/POP/IMAP (Simple Mail Transfer Protocol/Post Office Protocol/ Internet Message Access Protocol): Protocols for email communication.



➢ Communication and Web Technology:

Communication and web technology are closely intertwined, as web technology serves as the foundation for various forms of digital communication Web technology enables the creation, transmission, and reception of information and messages over the internet, transforming how individuals, businesses, and organizations communicate. Here's how communication and web technology intersect:

1. Email:

Email is a fundamental form of digital communication that relies on web technology. Web servers and email clients use protocols like SMTP (Simple Mail Transfer Protocol) and IMAP (Internet Message Access Protocol) to send, receive, and manage email messages. Web-based email services like Gmail and Outlook operate entirely within a web technology framework, allowing users to access their emails from anywhere with an internet connection.

2. Instant Messaging and Chat

Instant messaging applications and chat platforms, such as WhatsApp, Facebook Messenger, and Slack, are web based and utilize web technology to enable real-time communication. These platforms operate through web browsers and dedicated applications that leverage web protocols.

3. VoIP and Video Calls Technology

Voice over Internet Protocol (VoIP) and video conferencing services, such as Skype, Zoom, and Microsoft Teams, rely on web technology for communication. These services use web based protocols for audio and video transmission over the internet.

4. Social Media

Social media networks like Facebook, Twitter, and Instagram are built on web technology. They allow users to share text, images, videos, and links, and engage in online conversations through web-based interfaces.

5. Web Conferencing and Webinars

Web conferencing tools like Webex and GoToMeeting, as well as webinar platforms, enable remote meetings and presentations. These technologies use web- based communication protocols to facilitate collaboration and information sharing.

6. Blogs and Forums

Blogging platforms and online forums enable users to engage in discussions and share information. These platforms are web-based and use web technology to publish and access content.

7. Social Networking Sites

Platforms like LinkedIn and professional networking sites enable users to connect with others, share professional information, and communicate with peers and colleagues using web technology.

8. News and Media

News websites, online publications, and multimedia content providers use web technology to distribute news articles, videos, and multimedia content to a global audience.

9. Web Forms and Surveys

Web forms and survey tools facilitate data collection and feedback gathering through web-based interfaces. **Examples:** Google forms, feedback.

10. Online Collaboration

Collaborative tools, including project management software and document sharing services, rely on web technology for communication and real-time collaboration among team members.
Examples: Brainstorming (White board), software, Zoom, Microsoft teams.

➢ Internet:

The Internet can be defined as a large network that connects other networks of computers all around the world. An example of a single network of computers might be all the computers connected within an entire school district. The Internet is tens of thousands of these networks communicating with one another. Using different applications, such as e-mail, telnet and gopher. A user is allowed to interact with information found on the other computers connected to the Internet.

➢ Definition of Internet:

The internet is a global network of interconnected computers, servers, phones, and smart appliances that communicate with each other using the transmission control protocol (TCP) standard to enable a fast exchange of information and files, along with other types of services.

➢ How the Internet works:

- The internet is a network that connects thousands of individual computer networks. Each computer on the internet has a unique address. This address can be referred to as 'a number', which is called IP Address' or 'a name, is called 'Domain Name'. For example, IP Address: 192.65.245.76 and Domain Name: oregano.mwe.edu

- Everything that is sent across the internet is a 'packet' of data. Your e-mail, your live chats, your web searches and FTP sessions are all packets of data. The reason computers of vastly different manufacture can exchange data is due to a set of standards called 'Protocol'. Protocol is like rules that govern the exchange of information.

- These protocols make it possible for one computer to translate its data into a form readable to all computers and send the data out on its way.

- The two primary protocols of the internet are Transmission Control Protocol (TCP) and Internet Protocol (IP).

- TCP breaks your data up into small IP packets (which are numbered so receipt can be verified and the data put back in correct order) which are passed along from one network to another until they reach their destination. At the destination the TCP protocol reassembles the packets into the message.

- The internet is a **'packet-switch'** network. The emphasis is on exchanging packets of data rather than connecting computer systems together. When telnet is used, for example, it looks as though there is a direct connection between two computers. But it's a "virtual connection"; the two systems aren't really directly connected to each other. In reality packets are being passed from one system to another. The networks on the internet uses a hardware device called a **'Router'**.

- Many internet services and tools operate on a scheme called **'Client/Server'**. A person on one computer starts a program that contacts another (remote) computer. The 'Client' is the program the person is running on the first computer and the server is running on the remote computer. The person gives commands to his client software, which then passes the commands on to the server at the remote computer and the **'Server'** sends back the reply to the command. Usually, a server can deal with several clients. Gopher works this way, and IRC and the World Wide Web (WWW)

➢ Advantages of the Internet:

1. Online Banking and Transaction: The Internet allows us to transfer money online through the net banking system. Money can be credited or debited from one account to the other.

2. Education, Online Jobs, Freelancing: Through the Internet, we are able to get more jobs via online platforms like LinkedIn and to reach more job providers. Freelancing on the other hand has helped the youth to earn a side income and the best part is all this can be done via the INTERNET.

3. Entertainment: There are numerous options for entertainment online we can listen to music, play games can watch movies, and web series, and listen to podcasts, youtube itself is a hub of knowledge as well as entertainment.

4. New Job Roles: The Internet has given us access to social media, and digital products so we are having numerous new job opportunities like digital marketing and social media marketing online businesses are earning huge amounts of money just because the Internet is the medium to help us to do so.

5. Best Communication Medium: The communication barrier has been removed from the Internet. You can send messages via email, Whatsapp, and Facebook. Voice chatting and video conferencing are also available to help you to do important meetings online.

6. Comfort to humans: Without putting any physical effort you can do so many things like shopping online it can be anything from stationeries to clothes, books to personal items, etc. You can books train and plane tickets online.

7. GPS Tracking and google maps: Yet another advantage of the internet is that you are able to find any road in any direction, and areas with less traffic with the help of GPS on your mobile.

➢ Disadvantages of the Internet:

1. Time Wastage: Wasting too much time on the internet surfing social media apps and doing nothing decreases your productivity rather than wasting time on scrolling social media apps one should utilize that time in doing something skillful and even more productive.

2. Bad Impacts on Health: Spending too much time on the internet causes bad impacts on your health physical body needs some outdoor games exercise and many more things. Looking at the screen for a longer duration causes serious impacts on the eyes.

3. Cyber Crimes: Cyberbullying, spam, viruses, hacking, and stealing data are some of the crimes which are on the verge these days. Your system which contains all the confidential data can be easily hacked by cybercriminals.

4. Effects on Children: Small children are heavily addicted to the Internet watching movies, and games all the time is not good for their overall personality as well as social development.

5. Bullying and Spreading Negativity: The Internet has given a free tool in the form of social media apps to all those people who always try to spread negativity with very revolting and shameful messages and try to bully each other which is wrong.

➢ World Wide Web

History:

It is a project created, by Timothy Berner Lee in 1989, for researchers to work together effectively at CERN. is an organization, named the World Wide Web Consortium (W3C), which was developed for further development of the web. This organization is directed by Tim Berner’s Lee, aka the father of the web.

Working of WWW:

The World Wide Web is based on several different technologies: Web browsers, Hypertext Markup Language (HTML) and Hypertext Transfer Protocol (HTTP).

A Web browser is used to access web pages. Web browsers can be defined as programs which display text, data, pictures, animation and video on the Internet. Hyperlinked resources on the World Wide Web can be accessed using software interfaces provided by Web browsers. Initially, Web browsers were used only for surfing the Web but now they have become more universal. Web browsers can be used for several tasks including conducting searches, mailing, transferring files, and much more. Some of the commonly used browsers are Internet Explorer, Opera Mini, and Google Chrome.

The Language of the Web:

There are three main components to this language to communicate in the Web.

1. Uniform Resource Locators (URLs): URLs provide the hypertext links between one document and another. These links can access a variety of protocols (e.g., ftp, gopher or http) on different machines or your own machine.

2. Hypertext Markup Language (HTML): Hypertext Markup Language, a standardized system for tagging text files to achieve font, colour, graphic and hyperlink effects on World Wide Web pages.

3. Common Gateway Interfaces (CGI): CGIS provide a gateway between the HTTP server software and the host machine.

➢ Advent of Internet

The advent of the internet marked a revolutionary turning point in the way humanity communicates, accesses information, conducts business, and interacts with the world. The origins of the internet can be traced back to various developments and milestones:

1. Early Concepts (1960s)

The concept of a global network of computers was envisioned in the early 1960s. J.C.R. Licklider, an MIT scientist, conceived the idea of an **"Intergalactic Network"** of computers.

2. ARPANET (1969)

The Advanced Research Projects Agency Network (ARPANET) was the first wide-area packet-switching network, funded by the U.S. Department of Defense's ARPA. It became operational in 1969 and is considered a precursor to the modern internet.

3. Email and File Sharing (1970s)

Ray Tomlinson sent the first networked email in 1971, using the "@" symbol to designate sending messages between users on different machines. File Transfer Protocol (FTP) was introduced in 1971 for efficient file sharing.

4. TCP/IP Protocol (1970s)

The development of the Transmission Control Protocol (TCP) and Internet Protocol (IP) by Vinton Cerf and Bob Kahn in the 1970s was a crucial step toward the unification of various networks into a single global network of networks, forming the basis of the modern internet.

5. Ethernet and Local Area Networks (1970s)

Ethernet, developed by Robert Metcalfe, allowed multiple computers communicate on a local network. This technology laid the foundation for local areas networks (LANs) and facilitated the growth of interconnected networks.

6. DNS (1983)

The Domain Name System (DNS) was introduced to convert human-readable domain names into numerical IP addresses, making it easier to access websites.

7. World Wide Web (1991)

Tim Berners Lee, while working at CERN, proposed the World Wide Web (WWW), introducing HTML, HTTP, and the first web browser. This marked the birth of the user-friendly internet we are familiar with today.

8. Commercialization and Expansion (Mid-1990s)

The National Science Foundation (NSF) lifted restrictions on the commercial use of the internet, leading to a surge in internet service providers (ISPs) and a rapid increase in internet usage globally.

9. Dot-com Bubble (Late 1990s)

The late 1990s saw a massive rise in internet-based companies, leading to the dot-com bubble, where stock prices of internet companies soared before dramatically crashing in the early 2000s.

10. Broadband and High-Speed Internet (2000s)

The 2000s saw a widespread rollout of broadband internet, significantly improving internet speed and enabling new possibilities such as streaming media and online gaming.

11. Mobile Internet (2000s onwards)

The proliferation of smartphones and mobile devices brought internet access to s wider audience, revolutionizing communication, entertainment, and commerce.

12. Web 2.0 and Social Media (2000s onwards)

The advent of Web 2.0, characterized by user-generated content and interactive web applications, led to the rise of social media platforms like Facebook, Twitter. YouTube, and others, transforming how people connect and share information.

➢ Internet Infrastructure for Data Transfer and Governance:

The internet's infrastructure for data transfer and governance is a complex system of interconnected components and protocols that enable the transmission, exchange, and management of data globally. It encompasses both the physical and logical elements that facilitate data movement and the policies, standards, and organizations that govern its usage.

1. PHYSICAL INFRASTRUCTURE

The physical infrastructure of the internet comprises the tangible components that enable the transmission of data and the functioning of digital communication. These components include cables, data centers, network devices, and other hardware that make up the foundation of the internet. Here are the key elements of the physical infrastructure:

a) Submarine Cables

Fiber-optic cables laid on the ocean floor that connect continents and regions, forming the primary backbone of international internet connectivity.

b) Terrestrial Cables

Fiber-optic or copper cables that traverse land, connecting cities, towns, and regions. These cables form the backbone of national and regional internet networks.

c) Data Centers

Facilities that house network servers and other computing equipment. Data centers are critical for storing, processing, and managing vast amounts of data and services.

d) Network Servers

High-powered computers within data centers that store and serve data and applications to users across the internet.

e) Switches and Routers

Network devices that direct data packets to their intended destinations within a network or across networks. Routers operate at the network layer, making routing decisions based on IP addresses.

f) Firewalls and Security Appliances

Hardware devices that provide security by monitoring and controlling incoming and outgoing network traffic, protecting against unauthorized access and cyber threats & providing antivirus solution.

g) Modems and Routers in Homes and Businesses

Devices used to connect end user devices (computers, smartphones, IoT devices) to the internet via wired or wireless connections.

h) Satellite Communication Systems

Ground stations and satellites that facilitate internet connectivity in remote or geographically challenging areas where traditional infrastructure is impractical.

Types of Physical Infrastructure

a) Network Backbone: High speed, long-distance fiber optic cables and satellite links form the backbone of the internet, connecting continents and regions.

b) Internet Service Providers (ISPs): ISPs manage the last-mile connectivity to homes and businesses through wired (DSL, fiber, cable) and wireless (Wi-Fi mobile networks) technologies.

2. DATA TRANSMISSION PROTOCOLS

Data transmission protocols are a set of rules and conventions that govern the format, timing, sequencing, and error control during the exchange of data between devices over a network. These protocols ensure that data can be sent and received accurately and efficiently. Here are some important data transmission protocols:

a) Transmission Control Protocol (TCP)

TCP is a connection oriented protocol that provides reliable, ordered, and error checked delivery of data between devices. It establishes a connection, maintains flow control, and retransmits lost packets.

b) User Datagram Protocol (UDP)

UDP is a connectionless protocol that offers a faster but less reliable way to send data. It does not establish a connection and does not guarantee delivery, making it suitable for real-time applications like video streaming and online gaming.

c) Internet Protocol (IP)

IP is a network layer protocol responsible for routing packets across a network. IPv4 and IPv6 are the most common versions of IP. IPv6 has been developed to address the limitations of IPv4, primarily the limited number of unique addresses.

d) Hyper Text Transfer Protocol (HTTP)

HTTP is the foundation of data communication on the World Wide Web. It defines how messages are formatted and transmitted, and how web servers and browsers should respond to different commands.

e) HTTPS (HTTP Secure)

HTTPS is the secure version of HTTP, providing encrypted communication by using Secure Sockets Layer (SSL) or Transport Layer Security (TLS) protocols.

f) File Transfer Protocol (FTP)

FTP is a standard network protocol used to transfer files from one host to another over a TCP-based network like the internet.

g) Simple Mail Transfer Protocol (SMTP)

SMTP is used for sending emails between servers. It defines the message format and how the messages should be relayed between mail servers.

h) Post Office Protocol version 3 (POP3) and Internet Message Access Protocol (IMAP)

POP3 and IMAP are used by email clients to retrieve messages from a mail server. POP3 usually downloads and deletes the messages, while IMAP keeps the messages on the server.

3. OPEN STANDARDS AND PROTOCOLS

Open standards and protocols are universally agreed upon rules, conventions, and formats that enable interoperability, compatibility, and consistency in the functioning of systems, devices, and applications. These standards are openly available, transparent, and not owned by any specific entity, encouraging collaboration and innovation.

Here are important open standards and protocols in the realm of information technology:

1. Internet Protocol Suite (TCP/IP)

The foundation of the internet, TCP/IP is a suite of protocols governing communication over networks. It includes protocols like TCP, UDP, IP, ICMP, and more.

2. Hyper Text Transfer Protocol (HTTP) and HTTPS

HTTP is the fundamental protocol for transferring data on the World Wide Web HTTPS is the secure, encrypted version of HTTP, providing secure communication.

3. Simple Mail Transfer Protocol (SMTP)

SMTP is a standard for email transmission, specifying how emails are sent and received between mail servers.

4. File Transfer Protocol (FTP)

FTP is a standard protocol for transferring files between a client and a server on a network.

5. Domain Name System (DNS)

DNS is an essential standard for translating domain names into IP addresses, making internet resources accessible using human readable names.

6. Transport Layer Security (TLS) and Secure Sockets Layer (SSL)

TLS and SSL are cryptographic protocols that provide secure communication over a computer network. They are widely used to secure web browsing, email, and other internet-based applications.

7. Simple Network Management Protocol (SNMP)

SNMP is a standard protocol used for network management and monitoring d devices like routers, switches, and servers.

➢ Internet Society:

The Internet Society (ISOC) is a global nonprofit organization dedicated ensuring that the internet remains open, transparent, and accessible for everyone. li was founded in 1992 and has played a vital role in the development and governance of the internet as we know it today.

The Internet Society is committed to fostering a global internet for the public good. Its initiatives and activities aim to ensure that the internet continues to be a powerful force for positive change, innovation, and societal development while respecting the principles of openness and inclusivity.

➢ Roles and Objectives:

1. Advocacy for an Open Internet

ISOC advocates for policies and practices that support an open and accessible internet. They work to promote net neutrality, privacy, freedom of expression, and the free flow of information.

2. Standards and Protocols

ISOC actively contributes to the development and promotion of open internet standards and protocols through various working groups, such as the Internet Engineering Task Force (IETF).

3. Internet Governance

ISOC participates in internet governance discussions and initiatives, working to ensure that a multistakeholder approach guides decisions about the internet's future.

4. Capacity Building and Education

The organization provides training, resources, and educational programs to individuals and organizations to enhance their understanding of internet technologies, policies, and best practices.

5. Community Building

ISOC brings together a diverse community of stakeholders, including engineers, policy makers, academics, activists, and users, to collaborate on internet-related issues and initiatives.

6. Global Reach and Chapters

ISOC has a global presence through its chapters, which operate in various countries. These chapters contribute to local and regional discussions on internet issues and help implement ISOC's mission at the grassroots level.

7. Internet Hall of Fame

ISOC manages the Internet Hall of Fame, which recognizes and honors individuals who have made significant contributions to the development and advancement of the internet.

8. Research and Publications

ISOC conducts research and publishes reports on internet related topics, sharing knowledge and insights to inform policy discussions and technology advancements.

9. Community Grants and Funding

ISOC provides grants and funding to support projects and initiatives that align with their mission of an open, accessible, and secure internet.

➢ Regulation of Cyberspace:

Regulation of cyberspace involves the establishment and enforcement of rules, laws, and guidelines to govern behavior, activities, and transactions in the digital realm. Given the global nature of the internet, regulation often involves international cooperation, as well as efforts at national, regional, and organizational levels. Here are key aspects of regulating cyberspace:

1. Legislation and Laws

Governments enact laws to regulate various aspects of cyberspace, including data protection, privacy, cybersecurity, intellectual property rights, e-commerce, cybercrime, and freedom of expression. These laws set the legal framework and establish consequences for non-compliance.

2. International Agreements and Treaties

International cooperation is crucial to address global cybersecurity challenges Agreements and treaties between countries facilitate cooperation in combating cybercrime, sharing threat intelligence, and establishing norms for responsible behavior in cyberspace.

3. Regulatory Authorities

Regulatory bodies at national and regional levels oversee compliance with laws and regulations related to cyberspace. These authorities are responsible for enforcing rules, investigating violations, and imposing penalties on non-compliant entities.

4. Industry Standards and Best Practices

Industry-specific organizations and international bodies develop and promote standards and best practices for cybersecurity, privacy, data governance, and other relevant areas Compliance with these standards often becomes a requirement for organizations operating in specific sectors.

5. Data Protection and Privacy Regulations

Laws and regulations such as the European Union's General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) define how organizations collect, use, store, and share personal data, ensuring the privacy and rights of individuals.

6. Cybersecurity Regulations

Governments and industry bodies establish regulations to mandate cybersecurity measures, incident reporting, risk management, and secure software development practices to enhance overall cybersecurity posture.

7. Net Neutrality

Net neutrality regulations ensure that internet service providers treat all data on the internet equally, without discriminating or charging differently based on content, platform, application, or method of communication.

8. Critical Infrastructure Protection

Regulations aim to protect critical infrastructure sectors (e.g. energy, finance, healthcare) from cyber threats by setting security standards and requiring compliance to ensure operational resilience.

9. Internet Governance Organizations

Entities like the Internet Corporation for Assigned Names and Numbers (ICANN) and the Internet Engineering Task Force (IETF) play critical roles in coordinating and managing various aspects of the internet, contributing to its stability and security.

10. User Education and Awareness

Governments and organizations often engage in campaigns to educate users about safe online practices, privacy, and cybersecurity risks, aiming to promote responsible behavior in cyberspace.

➢ Meaning of Cyber Security:

Cybersecurity refers to the practice of protecting computer systems, networks, and digital infrastructure from theft, damage, unauthorized access, and other cyber threats. The primary goal of cybersecurity is to ensure the confidentiality, integrity, and availability of information, as well as to protect systems and data from various forms of cyberattacks.

➢ Definition of Cyber Security:

"Cyber Security is the body of technologies, processes, and practices designed to protect networks, devices, programs, and data from attack, theft, damage, modification or unauthorized access."

"Cyber Security is the set of principles and practices designed to protect our computing resources and online information against threats."

➢ Key Concepts in Cybersecurity:

1. **Confidentiality:** Protecting information from unauthorized access ensures that only authorized individuals or systems can access sensitive data.

2. **Integrity:** Maintaining the accuracy and reliability of data is essential. Cybersecurity measures aim to prevent unauthorized alteration of information.

3. **Availability:** Ensuring that information and resources are available when needed is a core principle. Cybersecurity strategies work to prevent disruptions and ensure continuous access to digital assets.

4. **Authentication:** Verifying the identity of users, devices, and systems is critical for controlling access to sensitive data and resources.

5. **Authorization:** Granting appropriate access privileges based on authenticated identities helps prevent unauthorized access to sensitive information.

6. **Non-repudiation:** This principle ensures that a user cannot deny their actions, providing accountability for digital transactions and activities.

7. **Digital Transactions:** Online activities like e commerce, social media, email and web browsing all take place within cyberspace. It is the platform for various digital services and transaction.

8. **Security Challenges:** Cyberspace is vulnerable to various cyber threats and security concerns, including hacking, malware, data breaches, and cyberattacks. As a result, cybersecurity is essential to protect the integrity and privacy of digital information.

➢ Issues of Cyber Security:

Cybersecurity encompasses a wide array of issues and challenges due to the complex and dynamic nature of the digital landscape. Here are some key issues in cybersecurity:

1. Cyber Threats and Attacks

Constantly evolving cyber threats include malware, ransomware, phishing, social engineering, denial-of-service (DoS) attacks, advanced persistent threats (APT), zero-day exploits, and more. Attackers continuously refine their tactics and tools, making it challenging to stay ahead.

2. Data Breaches

Data breaches expose sensitive information, such as personal records, financial data, and intellectual property. Breached data can be misused for identity theft, fraud, or sold on the dark web.

3. Identity Theft and Fraud

Stolen personal information is used for identity theft, leading to financial losses and reputational damage. Cybercriminals may open accounts, make purchases, or conduct other fraudulent activities in the victim's name.

4. Insider Threats

Malicious or negligent actions by employees, contractors, or partners pose a significant risk. Insiders can deliberately or accidentally compromise security, leak sensitive information, or engage in fraud.

5. IoT and OT Vulnerabilities

The proliferation of Internet of Things (IoT) and operational technology (OT) devices introduces new vulnerabilities, as many lack security features. Compromised IoT and OT devices can be leveraged for attacks or disrupt critical infrastructure

6. Supply Chain Risks

Supply chains involve multiple interconnected entities, making them susceptible to cyber attacks. Malicious actors may compromise software or hardware during production or distribution, introducing vulnerabilities or backdoors.

7. Lack of Security by Design

Inadequate consideration of security during the design and development phases of systems and applications results in vulnerabilities that may be challenging and costly to address later.

8. Human Error and Lack of Awareness

Employees and individuals often inadvertently contribute to security breaches through actions like clicking on phishing emails or using weak passwords Insufficient awareness and training exacerbate this issue.

➢ Challenges of Cyber Security:

Cybersecurity faces numerous challenges, reflecting the evolving nature of cyber threats, technological advancements, and the increasingly interconnected digital landscape. Here are some of the major challenges in cybersecurity:

1. Sophisticated Cyber Threats

Cyber attackers are continually improving their tactics, techniques, and procedures. Advanced persistent threats (APTs), ransomware, zero-day vulnerabilities, and polymorphic malware present significant challenges for cybersecurity professionals.

2. Evolving Attack Vectors

Attackers exploit various attack vectors, including phishing, social engineering. supply chain attacks, IoT vulnerabilities, and insider threats. New attack vectors continually emerge, making it difficult to predict and prevent all possible attack scenarios.

3. Data Breaches and Privacy Concerns

High-profile data breaches compromise sensitive personal and financial information, resulting in financial losses, identity theft, and reputational damage. Privacy regulations add complexity to compliance and require robust data protection measures.

4. Shortage of Skilled Cybersecurity Professionals

The demand for skilled cybersecurity professionals exceeds the available talent. A lack of skilled experts in areas like threat hunting, incident response, and security analysis poses a significant challenge for organizations seeking to enhance their security posture.

5. Legacy Systems and Infrastructure

Many organizations still rely on outdated legacy systems and infrastructure that may have inherent security vulnerabilities. Updating or replacing these systems is often costly, time-consuming, and complex.

6. Insider Threats and Human Error

Insiders with malicious intent or accidental actions by employees pose significant risks. Insider threats can be difficult to detect and prevent, making employee education, monitoring, and privileged access management crucial.

7. Compliance and Regulatory Changes

Keeping up with evolving cybersecurity regulations and compliance requirements is a challenge. Meeting various legal obligations across jurisdictions and industries demands dedicated resources and comprehensive understanding of relevant laws and standards

8. Integration of IoT and OT Security

The proliferation of Internet of Things (IoT) devices and operational technology (OT) in critical infrastructure introduces new security challenges. Securing these devices and integrating them into existing security frameworks is complex due to diverse architectures and protocols.

9. Nation-State Actors and Cyber Warfare

State-sponsored cyberattacks and cyber warfare pose significant threats to governments, critical infrastructure, and private sector organizations. The motivations include espionage, sabotage, and disruption of essential services.

10. Cybersecurity for Small and Medium-sized Enterprises (SMEs)

SMEs often lack the resources and expertise needed to implement robust cybersecurity measures. Attackers may target them as easier entry points into larger supply chains.

Nikitha S
Assistant Professor of Commerce
Basaveshwara College