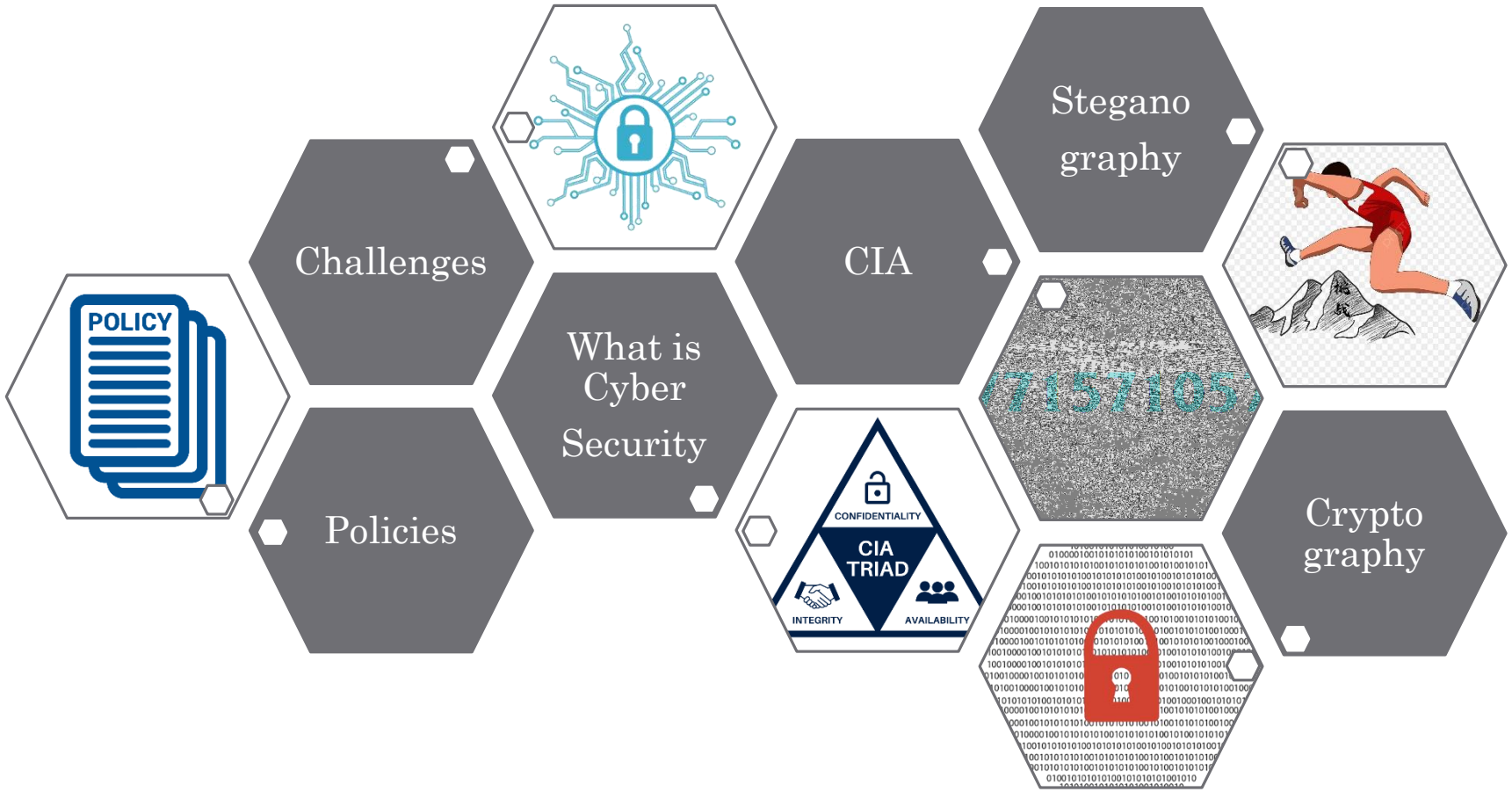
Cyber Security

By – Mr. Prathamesh Khade

Day – 1


POLICY
Challenges
What is Cyber Security
Policies
CIA
CONFIDENTIALITY
CIA TRIAD
INTEGRITY
AVAILABILITY
Stegano graphy
Crypto graphy

What is Cyber Security(CS)?

- Cybersecurity refers to the practice of protecting computer systems, networks, devices, and digital data from unauthorized access, theft, damage, or other malicious activities.
- Cybersecurity involves a range of practices, technologies, and measures that help to ensure the confidentiality, integrity, and availability of digital assets.
- Cybersecurity is important for businesses, governments, and individuals to prevent financial losses, data breaches, and other harmful effects that can result from cyber attacks.
- Cybersecurity threats can come from a variety of sources, including hackers, malware, phishing scams, and insider threats.
- Cybersecurity professionals work to stay up-to-date on the latest threats and vulnerabilities, and continually improve security measures to protect against these threats.

CIA Traid

- CIA triad is a well-known framework in cybersecurity that stands for confidentiality, integrity, and availability. The CIA triad is used to describe the three key objectives of cybersecurity, which are to protect the confidentiality, integrity, and availability of data and systems.
- The CIA triad is an essential framework for cybersecurity and is used by organizations of all sizes to help protect their assets and ensure the safety and security of their data and systems.
- The CIA triad helps organizations to identify potential vulnerabilities and risks, and to develop strategies and processes for addressing these risks to ensure the safety and security of their data and systems.

CS – Policies

- **Virus and Spyware Protection policy**
  - It helps to detect, removes, and repairs the side effects of viruses and security risks by using signatures.
- **Firewall Policy**
  - It blocks the unauthorized users from accessing the systems and networks that connect to the Internet.
- **Intrusion Prevention policy**
  - This policy automatically detects and blocks the network attacks and browser attacks. It also protects applications from vulnerabilities.
- **Application and Device Control**
  - This policy protects a system's resources from applications and manages the peripheral devices that can attach to a systems.

CS - Challenges

- Ransomware Evolution
- Blockchain Revolution
- IoT Threats
- AI Expansion
- Serverless Apps Vulnerability

ISO - 27001

- ISO 27001 is an international standard that provides a framework for establishing, implementing, maintaining, and continually improving an information security management system (ISMS).
- ISO 27001 is a globally recognized standard that provides a systematic and comprehensive approach to managing information security risks.
- ISO 27001 is applicable to organizations of all sizes, sectors, and types, including public and private organizations, non-profits, and government agencies.
- ISO 27001 certification is a formal recognition that an organization has implemented an ISMS in accordance with the requirements of the standard, and that it has demonstrated a commitment to continuously improving its information security practices.

Cryptography

- Cryptography is the practice of secure communication in the presence of third parties. It involves the use of mathematical algorithms and protocols to protect the confidentiality, integrity, and authenticity of digital data.
- There are two types of cryptography: symmetric cryptography, which uses the same key for encryption and decryption, and asymmetric cryptography, which uses different keys for encryption and decryption.

Steganography

- Steganography is the practice of concealing secret information within a non-secret medium in a way that prevents detection by unauthorized parties. It is often used in combination with cryptography to provide an extra layer of security.
- The goal of steganography is to make the hidden message as invisible as possible, so that it cannot be detected by anyone other than the intended recipient.
- Steganography is often used in combination with cryptography, which provides an additional layer of security by encrypting the message before it is hidden.

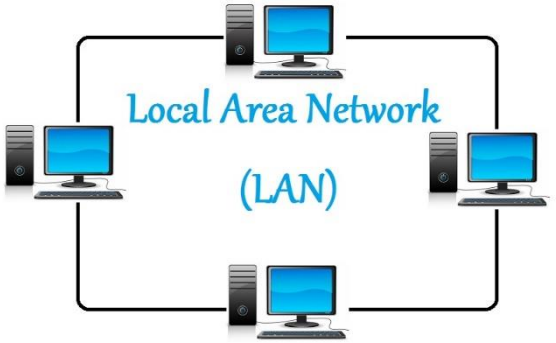
Network

- A network is a collection of computers, servers, and other devices that are interconnected to facilitate communication and resource sharing.
- In cybersecurity, networks are a critical component of an organization's infrastructure, and must be secured to protect against unauthorized access, data breaches, and other threats.
- Networks can be wired or wireless, and can be organized into different topologies, such as bus, ring, and star.
- Networks can be connected to the internet, which can provide access to a wide range of resources, but can also expose the network to a variety of cybersecurity threats.

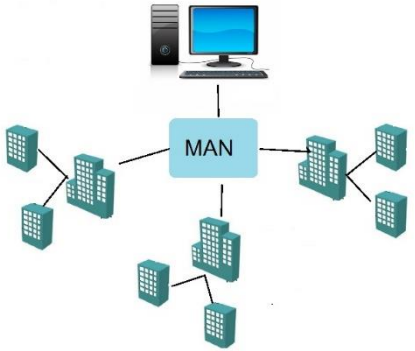
Networking Types

- Networking types refer to the different ways in which devices can be connected to form a network. There are several different networking types that are commonly used in the field of cybersecurity.
- LAN (Local Area Network): A LAN is a network that is confined to a small geographic area, such as an office building, school, or home.
- MAN (Metropolitan Area Network): A MAN is a network that covers a metropolitan area, such as a city or town.
- WAN (Wide Area Network): A WAN is a network that spans a large geographic area, such as a city, country, or even the entire world.
- There are several different types of network such as WLAN, PAN, CAN, SAN, VPN which are basically inherited from LAN, MAN & WAN.

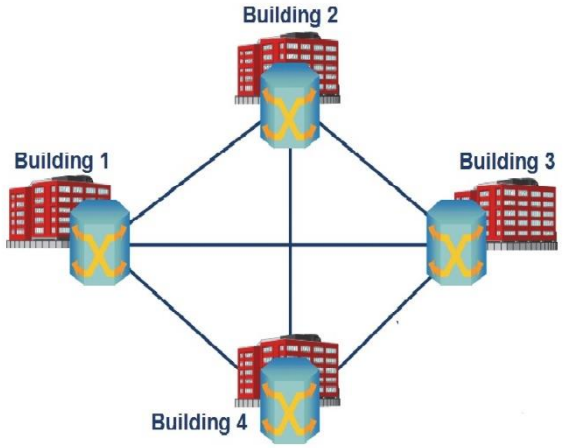
Pictorial Representation of Networking – Types.



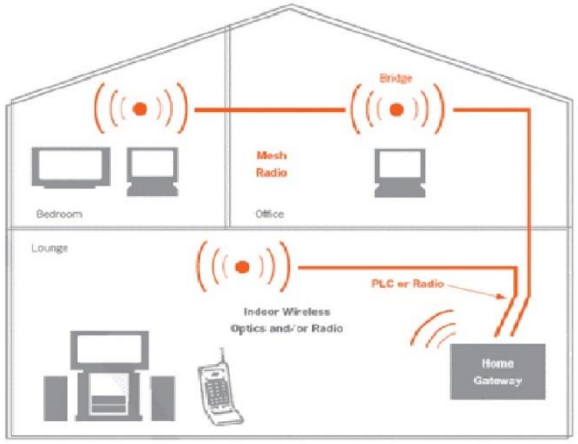
(WAN) Wide Area Network



Metropolitan Area Network



Campus Area Network(CAN)



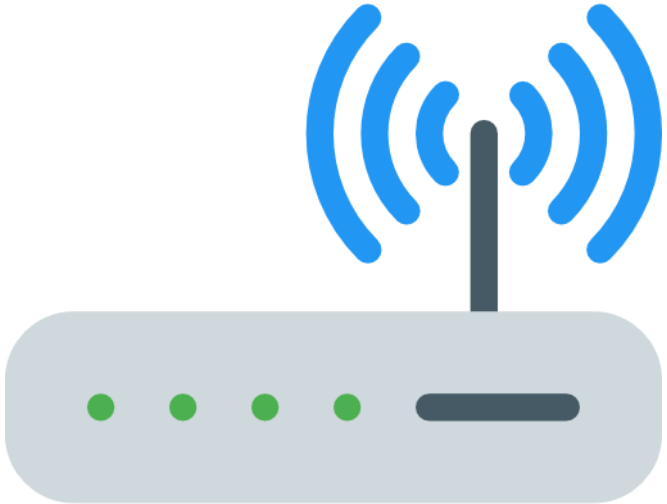
Home Area Network(HAN)

Network Devices

- Networking devices are hardware components that are used to facilitate communication and resource sharing between devices on a network.
- Some of the major networking devices includes:
  - Router
  - Switch
  - Firewall
  - NIC and many more…

Router

- A router is a networking device that is used to connect multiple networks together, such as a LAN and the internet.
- Routers use routing tables and protocols to determine the most efficient path for data to travel between networks.
- They also provide network address translation (NAT) services to translate between public and private IP addresses.



Switch

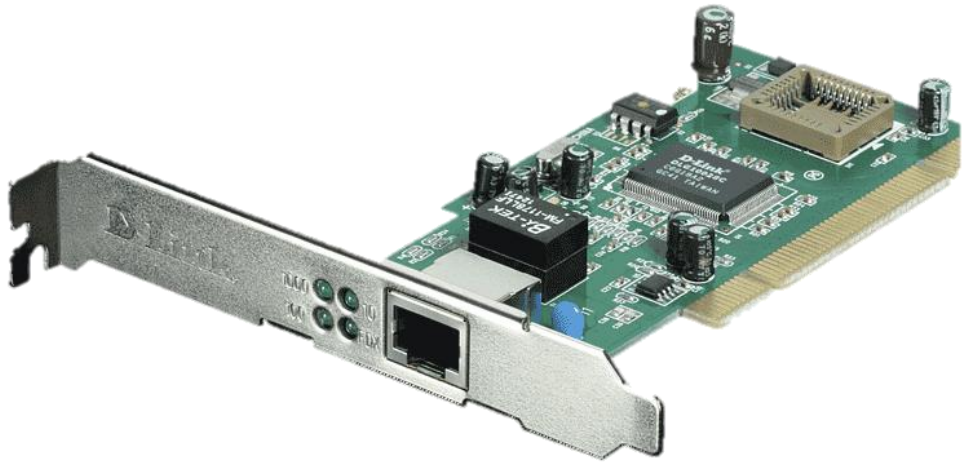
- A switch is a networking device that is used to connect multiple devices within a LAN.
- Switches use MAC addresses to forward data packets between devices on the same network.
- They are often used in conjunction with routers to provide local network connectivity.

Firewall

- A firewall is a networking device that is used to protect a network from unauthorized access and other security threats.
- Firewalls use a set of rules to filter incoming and outgoing network traffic.
- They can be configured to block certain types of traffic or to allow only authorized traffic to enter or leave the network.

Network Interface Card (NIC):

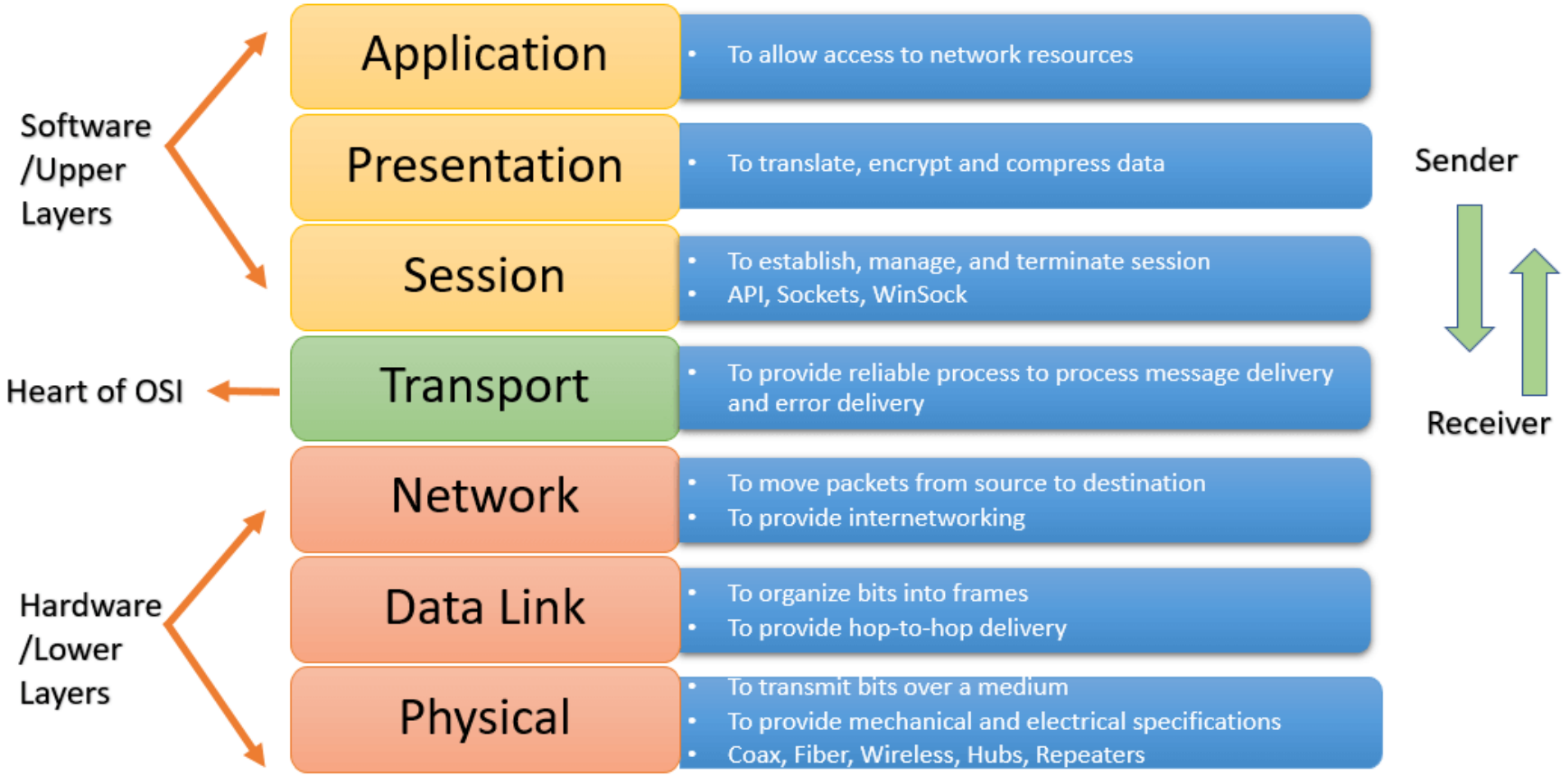
- A NIC is a hardware component that is used to connect a computer or other device to a network.
- NICs are often built into computers, but can also be installed as an expansion card.
- They provide a physical connection to the network and allow the device to communicate with other devices on the network.



Protocols

- Networking protocols are a set of rules and procedures that govern the communication between devices on a network.
- TCP/IP: TCP/IP (Transmission Control Protocol/Internet Protocol) is the primary networking protocol used on the internet and many other networks.
- DNS: DNS (Domain Name System) is a protocol used to translate human-readable domain names (such as google.com) into IP addresses that computers can understand
- DHCP: DHCP (Dynamic Host Configuration Protocol) is a protocol used to automatically assign IP addresses and other network configuration information to devices on a network.
- FTP: FTP (File Transfer Protocol) is a protocol used to transfer files between devices on a network. FTP servers allow users to upload and download files from a central location, and are commonly used to distribute software updates, documents, and other files.

OSI Model (Open Systems Interconnection Model)



Thank – You