CYBER SECURITY

UNIT 3: Basic Networking Concepts for Cyber Security

Networks and Their Importance

A network is a collection of devices connected to share data and resources. Cybersecurity depends heavily on networks because most data transfer occurs through them. Networks can be **LAN (Local Area Network)**, **WAN (Wide Area Network)**, or **PAN (Personal Area Network)**. IoT devices like smart home sensors, wearables, and industrial controllers rely on secure network connections to communicate with servers or cloud systems. Protecting networks ensures that data is transmitted safely and prevents attackers from intercepting sensitive information. Real-life examples include **banking networks**, where encrypted connections protect online transactions, and **smart city IoT networks**, where traffic and energy data are monitored securely.

OSI and TCP/IP Models

The **OSI (Open Systems Interconnection) model** has seven layers: Physical, Data Link, Network, Transport, Session, Presentation, and Application. Each layer has specific functions that help organize network communication and identify where security measures are needed. The **TCP/IP model** has four layers: Network Interface, Internet, Transport, and Application, and it forms the foundation of the internet. Understanding these models helps implement firewalls, intrusion detection, and encryption at appropriate points. For example, SSL/TLS protocols secure data at the Transport layer to protect online banking transactions.

Network Devices

Network devices include **routers, switches, hubs, and firewalls**. Routers direct traffic between networks, switches manage traffic within a network, and hubs broadcast data to multiple devices. Firewalls act as security barriers to block unauthorized access while allowing legitimate traffic. In IoT environments, routers and firewalls ensure that smart devices communicate securely without exposing private data. For instance, home routers with WPA3 encryption protect smart cameras and thermostats from hackers.

Internet Protocols

Internet protocols are rules that govern data transmission across networks. Common protocols include **HTTP, HTTPS, FTP, SMTP, and DNS**. HTTPS encrypts data between the browser and server, preventing attackers from reading sensitive information like login credentials or financial transactions. IoT devices use secure protocols like **MQTT and CoAP** for sending telemetry data to cloud servers safely. Misconfigured protocols can lead to data leakage or device hijacking. Real-life example: **smart healthcare systems** encrypt patient vitals transmitted from IoT monitors to hospital servers.

Network Security Issues

Network security issues arise from misconfigured devices, weak passwords, outdated firmware, or unpatched vulnerabilities. Attackers exploit these weaknesses using malware, phishing, or DDoS attacks. Public Wi-Fi networks are especially risky because data can be intercepted using packet sniffers or man-in-the-middle attacks. IoT devices are often targeted due to default passwords or unsecured communication channels. Real-life example: **Mirai botnet attack** in 2016 used insecure IoT devices to launch massive DDoS attacks, affecting global internet services.

Hackers and Threats to Networks

Hackers attempt to access networks illegally to steal data or disrupt services. White hat hackers test systems ethically, while black hat hackers exploit vulnerabilities for personal gain. Network threats include malware, ransomware, phishing attacks, and eavesdropping. Social engineering is commonly used to trick users into revealing passwords or confidential information. Real-life example: The **Colonial Pipeline attack** occurred because attackers accessed the network via compromised credentials, highlighting the importance of secure network access and monitoring.

Defense Mechanisms for Networks

Defense mechanisms protect networks using **firewalls, intrusion detection systems (IDS), intrusion prevention systems (IPS), VPNs, and encryption**. Firewalls filter traffic, IDS detects abnormal activity, and VPNs secure remote connections. Encryption ensures that intercepted data cannot be read by attackers. Layered security or **defense in depth** is essential because a single protective measure may not stop all attacks. For example, smart factories use multiple layers: network segmentation, encrypted data channels, and access control for IoT devices.

Monitoring and Maintenance

Continuous monitoring of network activity is crucial for early detection of attacks. Logs, alerts, and automated threat analysis tools help identify vulnerabilities before they are exploited. Regular firmware updates, patching, and password management prevent attacks on IoT devices and network infrastructure. Real-life example: **Google Cloud security monitoring** continuously scans for unusual network activity and automatically alerts administrators to potential threats.

Applications of Network Security

Network security is applied across industries to protect sensitive information and ensure uninterrupted operations. In healthcare, patient

data from IoT monitors must remain confidential. In banking, encrypted network communication protects online transactions. Smart homes, smart factories, and connected cars rely on secure network protocols to prevent data breaches and hacking. Proactive network security minimizes financial loss, reputation damage, and operational disruption while enabling safe IoT integration and cloud services.

Made with 💗 by Sagar Sangam

DIPLOMA WALLAH