CYBER SECURITY

UNIT 2: Introduction and Basic Concepts of Cyber Security

Cyber Security Overview

Cyber security is the practice of protecting computers, networks, programs, and data from unauthorized access, attacks, or damage. It ensures that sensitive information remains confidential, accurate, and available only to authorized users. Core security principles include **CIA — Confidentiality, Integrity, and Availability**, which guarantee that data is protected from theft, alteration, or loss. Another important model is **AAA — Authentication, Authorization, and Accounting**, which verifies user identity, controls access rights, and records activities. Vulnerabilities are weaknesses in systems that can be exploited by attackers, threats are potential dangers to data, and risks are the probability of an attack causing harm. Cyber attacks can include malware, phishing, ransomware, and Denial-of-Service (DoS) attacks, which disrupt services or steal data. Organizations use technology, processes, and trained personnel to protect systems, following frameworks like **McCumber Cube**, which combines people, technology, and policies for comprehensive security. Cyber security applies across infrastructure, networks, cloud services, IoT devices, and applications, helping businesses, governments, and individuals remain safe in a highly connected digital world. The evolution of cyber security has moved from simple antivirus programs to advanced threat detection systems and AI-based monitoring to tackle sophisticated attacks globally.

Networks and Security Models

Networks are the backbone of cyber security because they carry sensitive data between devices and systems. Understanding **OSI and TCP/IP models** helps in identifying where security measures must be applied. OSI model has seven layers that organize network functions, while TCP/IP model is simpler with four layers used in internet communication. Network devices like routers, switches, and firewalls help route, control, and protect data traffic. Firewalls monitor incoming and outgoing data and block unauthorized access, while hubs and switches manage device connections. Internet protocols like HTTP, HTTPS, FTP, and SMTP dictate how data is transmitted securely across networks. Network security issues can arise from misconfigured devices, weak passwords, or unpatched software. Real-life examples include **banking networks** where firewalls prevent unauthorized transactions and **IoT smart homes** where routers and encrypted Wi-Fi protect connected devices.

Hackers and Hacking Methodologies

Hackers are individuals or groups who attempt to access systems illegally for financial gain, espionage, or disruption. Not all hacking is illegal; ethical hackers test systems for vulnerabilities to improve security. There are different types of hackers — white hat, black hat, and grey hat — each with distinct motives. Hacking methodologies include phishing, password cracking, social engineering, and malware attacks. The famous **Stuxnet case** is a notable example, where a malicious worm targeted Iranian nuclear centrifuges, disrupting operations without physical intrusion. Understanding hacker behavior is critical for designing preventive measures, including monitoring, patching systems, and training personnel.

Malware and Cyber Attacks

Malware is software designed to harm or exploit devices and networks. Types include viruses, worms, Trojans, spyware, ransomware, and rootkits. Spyware collects personal information without consent, ransomware locks systems demanding payment, and backdoors provide secret access to attackers. Symptoms of attacks include slow system performance, unexpected pop-ups, unauthorized transactions, or system crashes. Infiltration methods often involve social engineering techniques such as pretexting, tailgating, or quid-pro-quo attacks. Denial-of-Service

(DoS) or Distributed DoS (DDoS) attacks overload servers to make services unavailable. Botnets are networks of compromised devices used to launch large-scale attacks. On-path attacks intercept data in transit between sender and receiver. Real-life examples include the **WannaCry ransomware attack**, which affected hundreds of thousands of computers worldwide, including healthcare systems, causing service disruption and financial loss.

Defense in Depth

Defense in depth is a layered security strategy that uses multiple protective measures to secure systems. Layers may include host encryption, antivirus software, firewalls, email gateways, honeypots, password management, and multi-factor authentication. This approach ensures that if one layer fails, others still protect the system. For example, a smart factory with IoT sensors may use encrypted data transmission, network firewalls, and access controls simultaneously to prevent cyber attacks. Security vulnerabilities can also arise in hardware and software, as seen in **Meltdown and Spectre**, which exploited CPU design flaws to access sensitive memory. Software vulnerabilities can be mitigated through regular updates, patches, and categorizing vulnerabilities to prioritize critical fixes. Advanced Persistent Threats (APTs) are prolonged and targeted attacks on high-value systems, often bypassing basic security layers using sophisticated techniques.

Data Maintenance and Safe Computing

Cybersecurity also includes data maintenance and safe computing practices. Backing up data, permanently deleting unneeded files, and understanding terms of service for apps are essential. Individuals must check privacy policies to know who owns their data and how it can be used. Firewalls, antivirus, and antispyware software protect devices, while managing operating systems and browsers reduces vulnerabilities. Using strong passwords, two-factor authentication, and secure networks prevents unauthorized access. For example, hospitals using IoT medical devices encrypt patient data and restrict access to authorized personnel only. Safeguarding online privacy also includes careful social sharing, email and browser privacy settings, and monitoring risky behavior like using public Wi-Fi for sensitive tasks. Tools like “Have I Been Pwned” help users check if their credentials are compromised.

Importance and Applications of Cyber Security

Understanding cyber security fundamentals, including CIA, AAA, threats, vulnerabilities, and defense mechanisms, prepares individuals and organizations to protect sensitive data effectively. From networks and IoT systems to cloud services and applications, applying these principles reduces the risk of financial loss, reputational damage, and legal consequences. Real-life examples such as **Amazon Web Services security**, **smart city IoT protections**, and **banking network firewalls** demonstrate how layered cybersecurity strategies work globally. Proactive monitoring, regular updates, ethical hacking, and user awareness are key elements in maintaining robust security across personal, organizational, and IoT environments.

Made with 💗 by Sagar Sangam

DIPLOMA WALLAH