Network Design and Management ITNT412

8. Network Security Design

CHAPTER 8

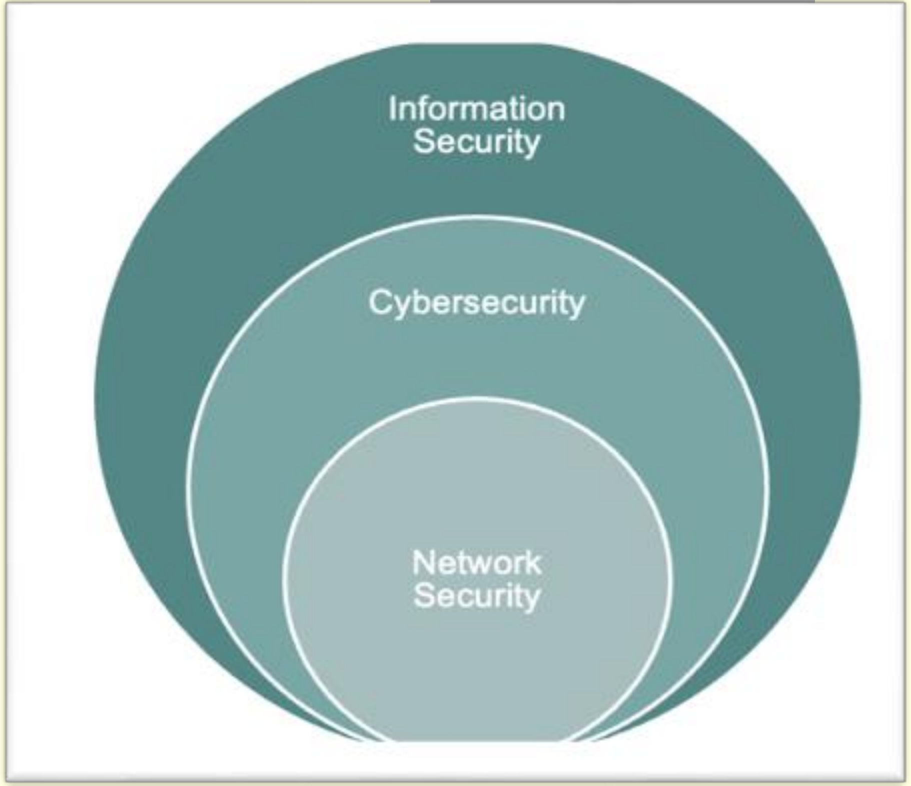
Dr. Mahmud Mansour

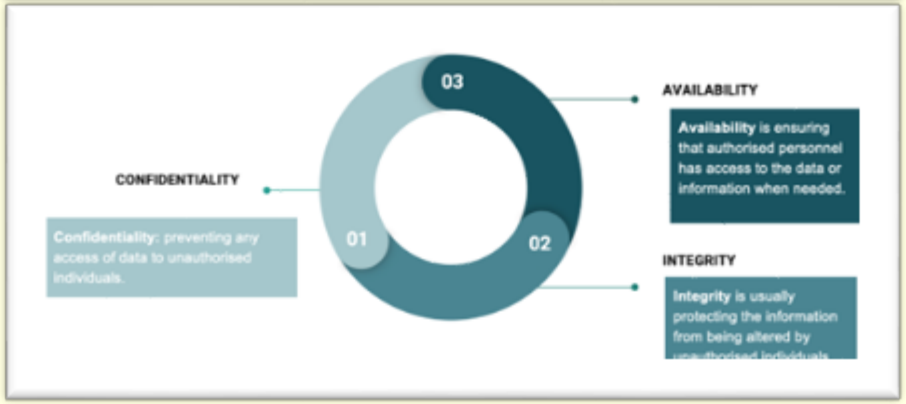
Information Security vs Cybersecurity vs Network Security

Information Security: is the measures taken to protect the information from unauthorized access and use. It provides confidentiality, integrity, and availability. It is the superset that contains cyber security and network security. It is necessary for any organization or firm that works on a large scale.

Cyber Security: Cybersecurity is the method of protecting systems, networks, and programs from digital attacks. Cybersecurity involves techniques that help and secure various digital components Networks, data, and computer systems from Unauthorized digital access.

Network Security: Network security is described as the implementation of techniques, processes, and protocols to protect the communication and information of an individual or organization.





Confidentiality: preventing any access of data to unauthorised individuals.

Availability is ensuring that authorised personnel has access to the data or information when needed.

Integrity is usually protecting the information from being altered by unauthorised individuals

Cybersecurity vs Network Security vs Information Security

S.No.	Cyber Security	Network Security	Information Security
01.	Cybersecurity is the method of protecting systems, networks, and programs from digital attacks.	Network Security is the method of protecting the usability and integrity of your network and data.	Information security is the measures taken to protect the records from unauthorized entry and use.
02.	Cyber Security is a subpart of Information Security.	Network Security is a subpart of Cyber Security.	Cyber Security & Network Security comes under Information Security.
03.	It protects anything in the cyber area.	It protects anything in the network area.	Information security is for information irrespective of the space.
04.	It deals with protection from cyber attacks.	It deals with protection from DOS (Denial of Service) attacks.	It deals with the security of data from any kind of threat.
05.	Cyber security attacks against cybercrime and cyber fraud.	Network Security attacks against trojans.	Information Security attacks against unauthorized access, disclosure modification, and disruption.
06.	Cyber security ensures the security of the entire digital data.	Network security only ensures the security of transit data.	Information security ensures the protection of transit and digital data.
07.	It deals with the security of the data resting.	It secures data traveling across the network by terminals.	It gives integrity, confidentiality, and availability.
08.	Common Cyber Security Risks: • Social engineering • Brute force • Baiting • Ransomware	Common Network Security Risks: • Viruses, worms, and trojans • Denial of Service (DOS) attack • Zero-day attacks	Common Information Security Risks: • Access • Destruction • Availability

Process of security design

- Identify network assets.
- Analyze security risks.
- Analyze security requirements and tradeoffs.
- Develop a security plan.
- Define a security policy.
- Develop procedures for applying security policies.
- Develop a technical implementation strategy.
- Train users, managers, and technical staff.
- Implement the technical strategy and security procedures.
- Test the security and update it if any problems are found.
- Maintain security.

Process of security design -1

- Identify network assets.
  - Including the hosts' operating systems, applications, and data, internetworking devices (such as routers and switches), and network data that traverses the network. also include intellectual property, trade secrets, and a company's reputation.
- Analyze security risks.
  - Risks can range from hostile intruders to untrained users who download Internet applications that have viruses.
  - Hostile intruders can steal data, change data, or delete data and cause service to be denied to legitimate users.
  - Denial-of-service (DoS) attacks have become increasingly common in the past few years

Process of security design -2

- Analyze security requirements and tradeoffs

The basic requirements need to develop and select procedures and technologies that ensure the following:

- The confidentiality of data, so that only authorized users can view.
- The integrity of data, so that only authorized users can change.
- Detect intruders and isolate the amount of damage they do.
- Protect data transmitted to remote sites across a VPN.
- Protect applications and data from software viruses
- Authenticate routing-table updates received from internal or external routers.
- System and data availability.

Process of security design -3

Analyze security requirements and tradeoffs

- Let outsiders (customers, vendors, suppliers) access data on public web or File Transfer Protocol (FTP) servers but not access internal data.
- Physically secure hosts and internetworking devices.
- Tradeoffs must be made between security goals and goals for affordability, usability, performance, and availability.
- Achieving security goals means making tradeoffs.
- Train network users and network managers on security risks
- Meet compliance and regulatory requirements

Process of security design -4

- Develop a security plan.
  - It is a high-level document that proposes what an organization is going to do to meet security requirements.
  - The time, The people, and other resources that will be required to develop a security policy.
  - A security plan should reference the network topology and include a list of network services that will be provided.

Process of security design -5

- Define a security policy.
  - A security policy is a formal statement of the rules and information assets must abide.
  - A security policy informs users, managers, and technical staff of their obligations for protecting technology and information.
  - The policy should specify the mechanisms by which these obligations can be met.
- Develop procedures for applying security policies.
  - Security procedures implement security policies.
  - Procedures define configuration, login, audit, and maintenance processes.
  - Should be written for end users, network administrators, and security administrators
  - Specify how to handle incidents.

Modularizing Security Design

In general, using a modular approach to security design is a good way to gain an understanding of the types of solutions that must be selected to implement security defense in depth:

- Internet connections
- Remote-access and virtual private networks (VPN)
- Network services and management
- Server farms
- User services
- Wireless networks

Internet connections

- Should be secured with a set of overlapping security mechanisms, including firewalls, packet filters, physical security, audit logs, authentication, and authorization.

- Internet routers should be equipped with packet filters to prevent DoS and other attacks.

- Select a protocol that offers route (OSPF-EIGRP-RIPv2) authentication.

Securing Remote-Access and VPNs

- Remote users and remote routers that use the Point-to-Point Protocol (PPP) should be authenticated with CHAP.
- Organizations use VPNs to connect private sites and end users via a public.
- IP Security Protocol (IPsec) the most common solution for encryption is to use.
- IPsec provides a secure path between remote users and a VPN concentrator, and between remote sites and a VPN site-to-site gateway.

Securing Network Services and Network Management

- Routing updates not accept from a router that has not been authenticated.
- Login IDs and passwords should be required for accessing routers and switches.
- Limiting use of the Simple Network Management Protocol (SNMP) should be considered on enterprise networks
- The main issues with SNMP is the **set** operation, which allows a remote station to change management and configuration data.
- If SNMPv3 is used, this is not as big a concern, because SNMPv3 supports authentication for use with the **set** operation and other SNMP operations.
- Network management systems should be especially protected because they host extremely sensitive data about network and security device configuration.
- To minimize risk, network management systems should be placed in their own DMZ behind a firewall.

Securing Server Farms

- Servers often contain an enterprise's most sensitive information.
- Server farms must be protected,Because are accessed by a large number of users.
- methods should be deployed to protect against the compromise of exposed applications and unauthorized access to data.
- To manage this risk, configure network filters that limit connectivity from the server.
- In many cases, a server has no need to initiate connections, Connection establishments generally come from the client

Securing User Services

- Specify which applications are allowed to run.
- Restrict the downloading of unknown applications from the Internet.
- PCs must have personal firewall and antivirus software installed.
- Users should be encouraged to log out of their sessions with servers when leaving their desks for long periods of time
- Automatic logouts can also be deployed

Securing Wireless Networks

- *Data privacy in wireless networks*
- *Authentication in wireless networks*

Type of user:

- Guests who visit an enterprise.
- Employees.

- EEE 802.11 specifies two forms of authentication: open and shared key, Wired Equivalent Privacy (WEP).