NETWORK SECURITY ESSENTIALS

BCA – IV

Credits – 4

Evaluations – 5

The course is designed to build an understanding of various network security components, protocols and creating the awareness about the issues due to security.

Pre-requisites: An understanding of Basic Computer Networking and security

UNIT 1

- Security Attacks (Interruption, Interception, Modification and Fabrication)
- Security Services (Confidentiality, Authentication, Integrity, Non-repudiation, access Control and Availability) and Mechanisms
- Model for Network Security
- Malicious Software: Viruses, Worms, Virus Defence, Trojan Horses
- Peer-to-Peer Security, Web Security, Dos, disk Encryption.

WHAT IS..

Information

Network

Risk

Threat

Opportunity

Network security

VARIOUS ASPECTS OF SECURITY

Physical Security - to protect the physical items, objects, or areas of an organization from unauthorized access and misuse.

Personal Security – to protect the individual or group of individuals who are authorized to access the organization and its operations.

Operations Security – to protect the details of a particular operation or series of activities.

Communications Security – to protect an organization’s communications media, technology, and content.

Network Security – to protect networking components, connections, and contents.

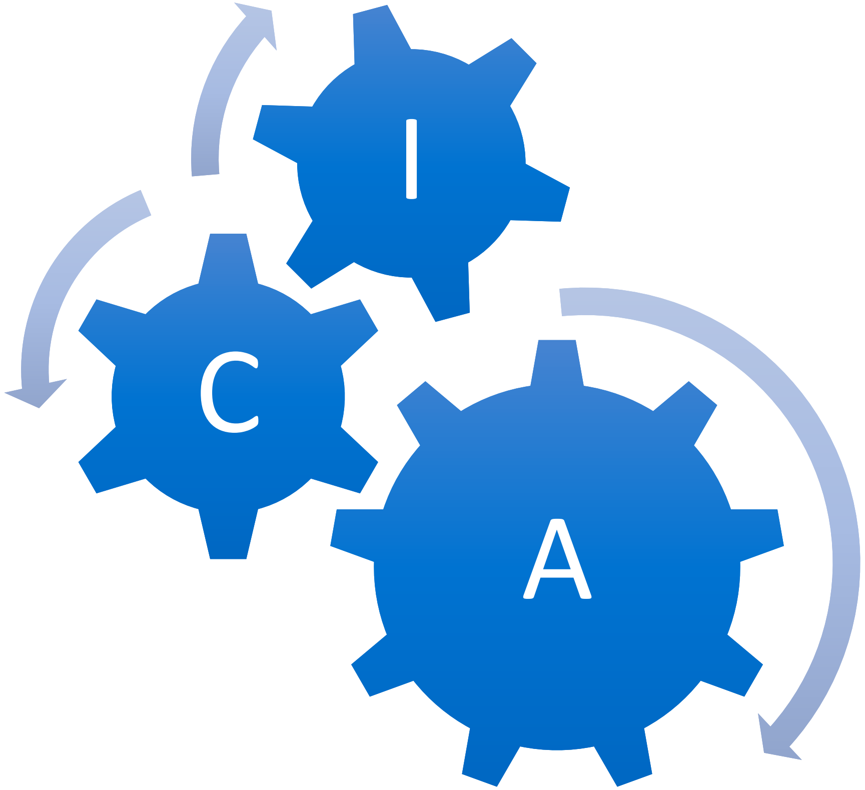
Information Security – to protect information assets

CIA Triad:

1. **Confidentiality**
   ensures information is inaccessible to unauthorized people

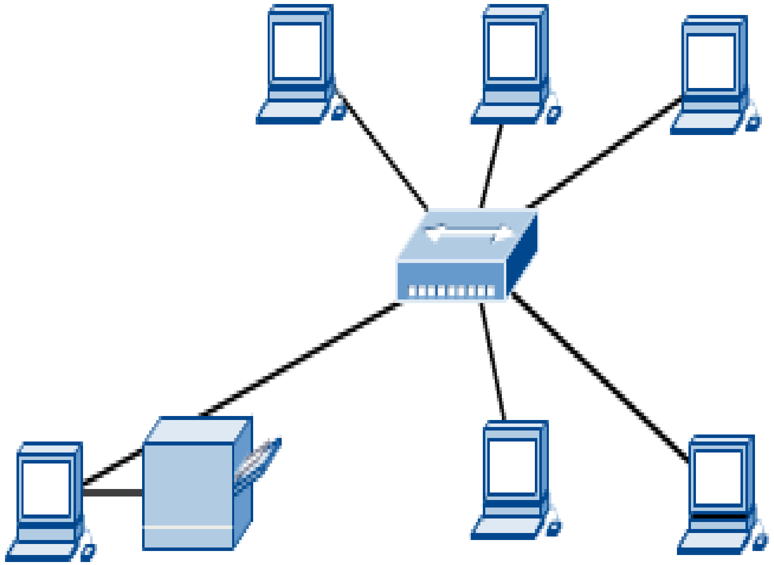
2. **Integrity**
   ensures the data is accurate and trustworthy by preventing unauthorized modification

3. **Availability**
   ensures authorized people can access the information when needed



What is a computer network?

- **Set of nodes connected by communication links.**
- **Computer network connects two or more autonomous computers.**
- **The computers can be geographically located anywhere.**



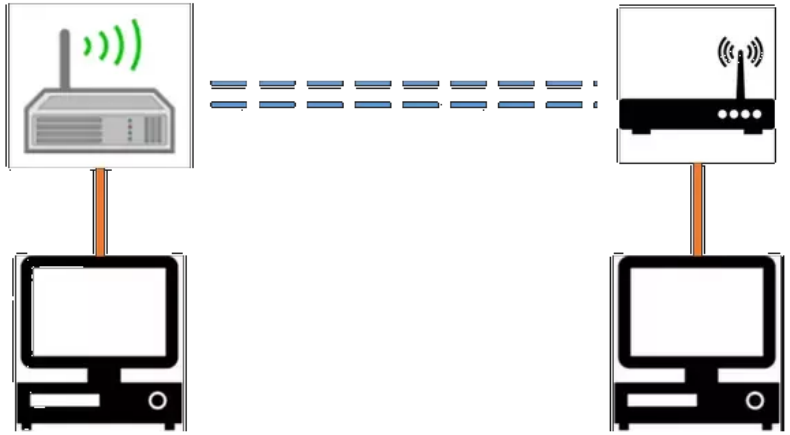
Nodes and Links

- Nodes - Node is a device capable of sending/receiving data generated by other nodes in the network.

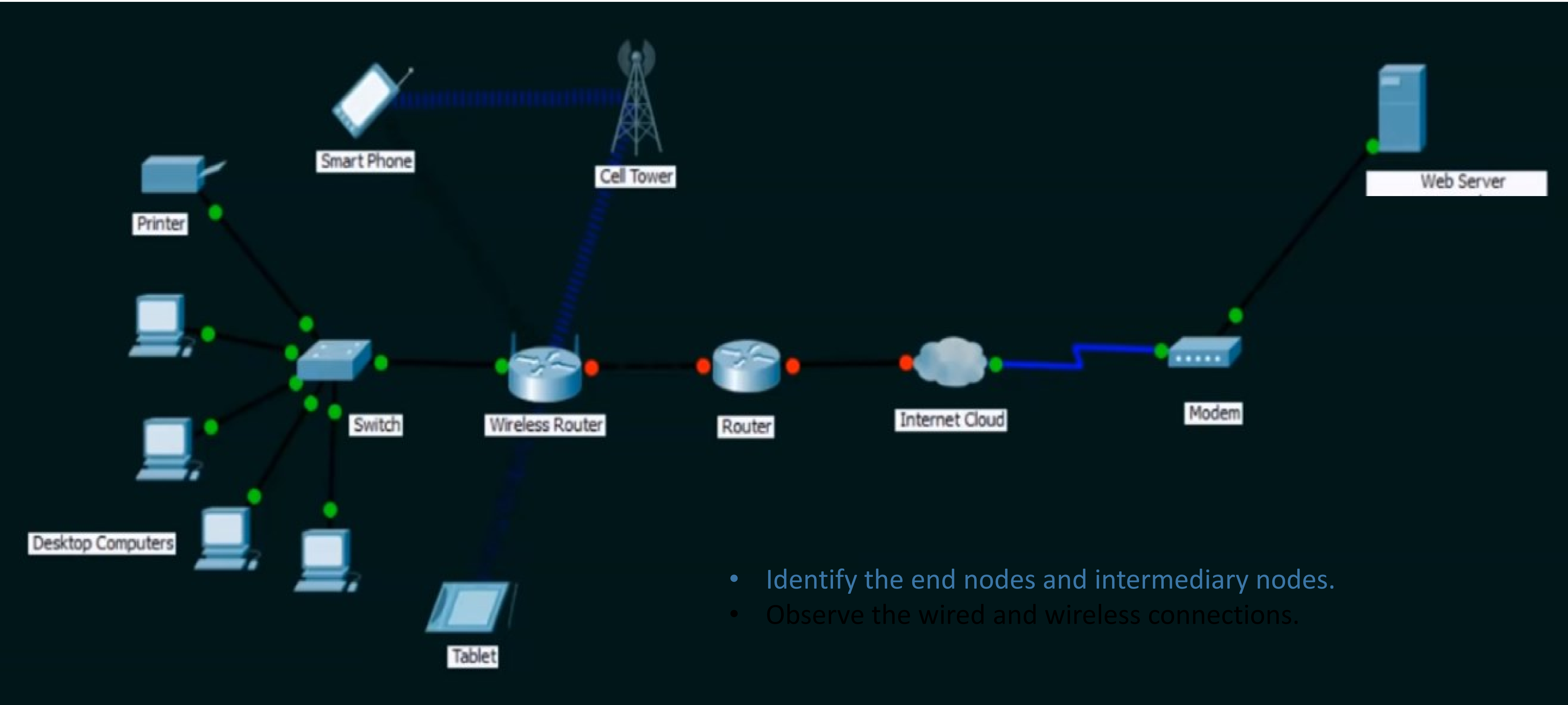
E.g. Computer, Server, Printer, Switch/Hub, Router

1. Is a security camera a node?
2. Is IP phone a node?

- Communication Link – A link between the nodes, wired or wireless.
- Link carries the information from one node to another.



Example of a network



- Identify the end nodes and intermediary nodes.
- Observe the wired and wireless connections.

APPLICATIONS, OBJECTIVES, AND ADVANTAGES OF NETWORK

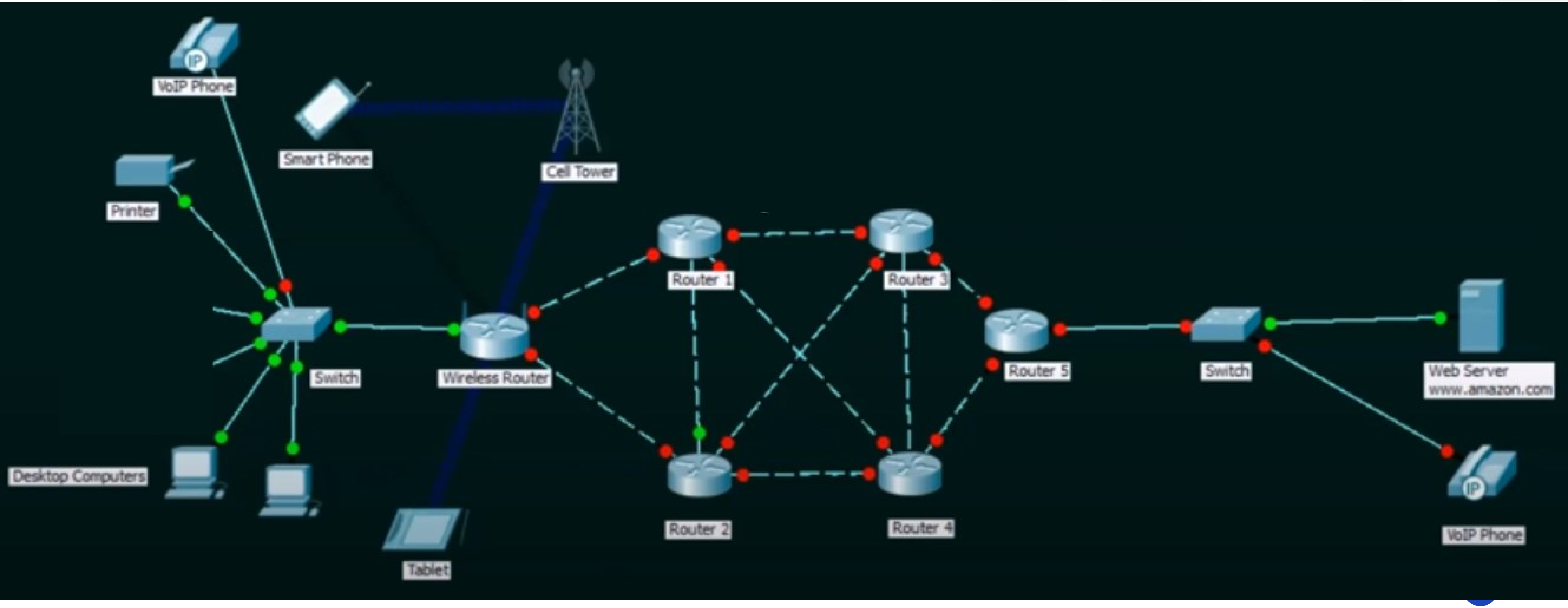
- **Resource Sharing**
  - Hardware (computing resources, disks, printers)
  - Software (application software)
- **Information Sharing**
  - Easy accessibility from anywhere (files, databases)
  - Search Capability (WWW)
- **Communication**
  - Email
  - Message broadcast
- **Remote computing**
- Backups

- Cost effective
- Independent of physical location – dependent on physical location (as required)
- High reliability and availability
- Load balancing
- Security

CHARACTERISTICS OF NETWORK

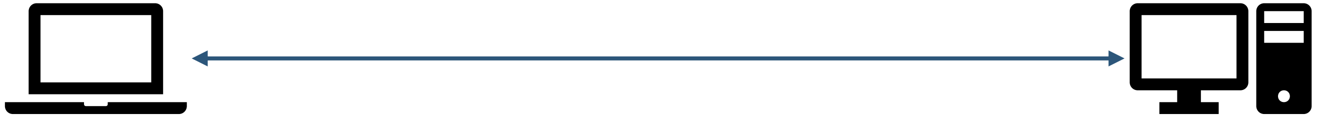
- **Fault Tolerance**
  - Ability to continue working despite failures
  - Ensure uninterrupted/continued service
- **Scalability**
  - Add/remove devices as required
  - Good performance after growth
- **Quality of Service (QoS)**
  - Ability to set priorities
  - Manage data traffic to reduce data loss/delay etc.
- **Security**
  - Prevent unauthorized access, misuse, forgery
  - Provide confidentiality, integrity, availability

1. Fault Tolerance (e.g. Link Failure)
2. Scalability (e.g. Internet)
3. Quality of Service (QoS)
4. Security



WHAT IS DATA COMMUNICATION?

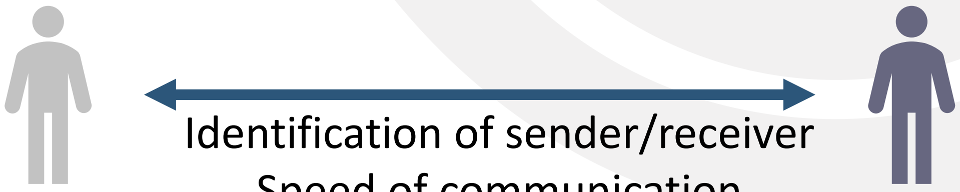
- Exchange of data between two nodes via a link or medium.



- Types of data flow
  - Simplex (define)
  - Half duplex (define)
  - Duplex (define)

PROTOCOLS

- What are protocols?
  - Protocols govern the methods of communication
- What if there are no protocols?
- Protocol determines
  - What is communicated?
  - How is it communicated?
  - When it is communicated?

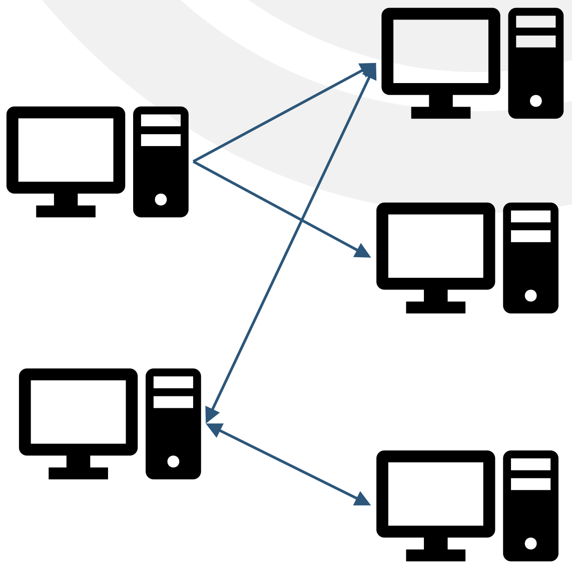


Identification of sender/receiver
Speed of communication
Language of communication
Confirmation/acknowledgement

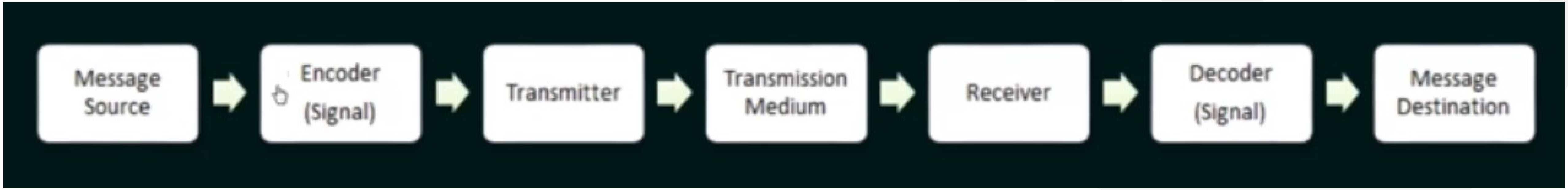
PROTOCOLS IN COMPUTER NETWORK

Elements of protocol:

- Message encoding
- Message formatting and encapsulation
- Message timing
- Message Size
- Message Delivery options



MESSAGE ENCODING



Message Source → Encoder (Signal) → Transmitter → Transmission Medium → Receiver → Decoder (Signal) → Message Destination

Encoding depends upon the type of medium. Electric/optical signal for wired medium, waves for wireless medium.

Message Formatting & Encapsulation

Agreed format for the sender and receiver

We add certain information to the message, e.g. information about sender and receiver

MESSAGE SIZING

Large data is broken down into small packets for quick transmission.
The size of packets depend in the capacity of medium.

e.g. large box transported from one location to another

Message Timing

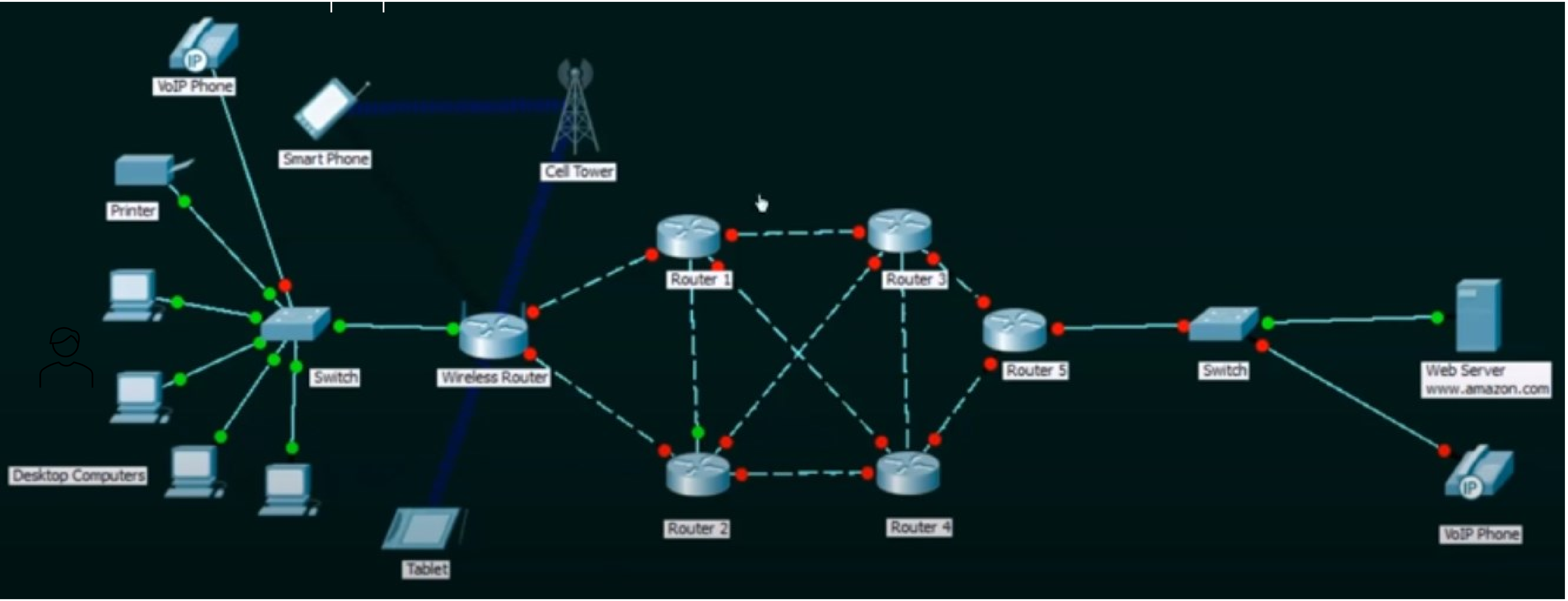
Flow control
Response timeout

Message Delivery Options

Unicast - One sender One receiver in a network
Multicast - One sender One Group of receivers in a network
Broadcast - One sender and All others are receivers

Example of Protocols

Message encoding
Message formatting & encapsulation
Message Size
Message timing
Message delivery option



THE NEED FOR INFORMATION SECURITY:

The purpose of data security management is to make sure business continuity and scale back business injury by preventing and minimizing the impact of security incidents. The basic principle of Information Security is:

- Confidentially
- Authentication
- Non-Repudiation
- Integrity

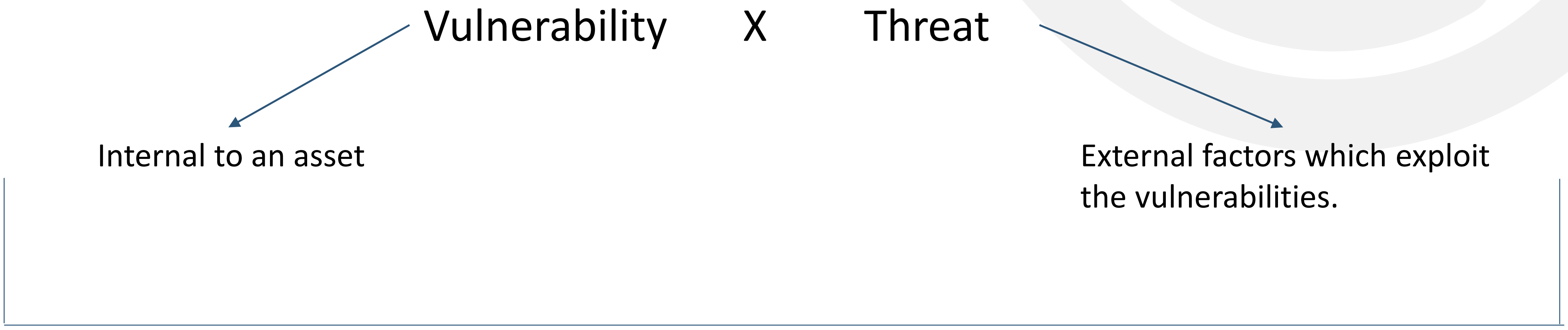
1.Protecting the functionality of the organization:
The decision maker in organizations must set policy and operates their organization in compliance with the complex, shifting legislation, efficient and capable applications.

2.Enabling the safe operation of applications:
The organization is under immense pressure to acquire and operates integrated, efficient and capable applications. The modern organization needs to create an environment that safeguards application using the organizations IT systems, particularly those application that serves as important elements of the infrastructure of the organization.

3.Protecting the data that the organization collects and use:
Data in the organization can be in two forms that are either in rest or in motion, the motion of data signifies that data is currently used or processed by the system. The values of the data motivated the attackers to seal or corrupts the data. This is essential for the integrity and the values of the organization's data. Information security ensures protection of both data in motion as well as data in rest.

4.Safeguarding technology assets in organizations:
The organization must add intrastate services based on the size and scope of the organization. Organizational growth could lead to the need for public key infrastructure, PKI an integrated system of the software, encryption methodologies. The information security mechanism used by the large organization is complex in comparison to a small organization. The small organization generally prefers symmetric key encryption of data.

ANALYZE THE RISK



Vulnerability X Threat

Internal to an asset

External factors which exploit the vulnerabilities.

Understand the vulnerabilities & threats which might affect of your network

THREATS AND VULNERABILITIES

Threats

- It is an external *agent* (person or thing) likely to cause damage
- Danger posed by someone else
- Can be identified but can’t be controlled

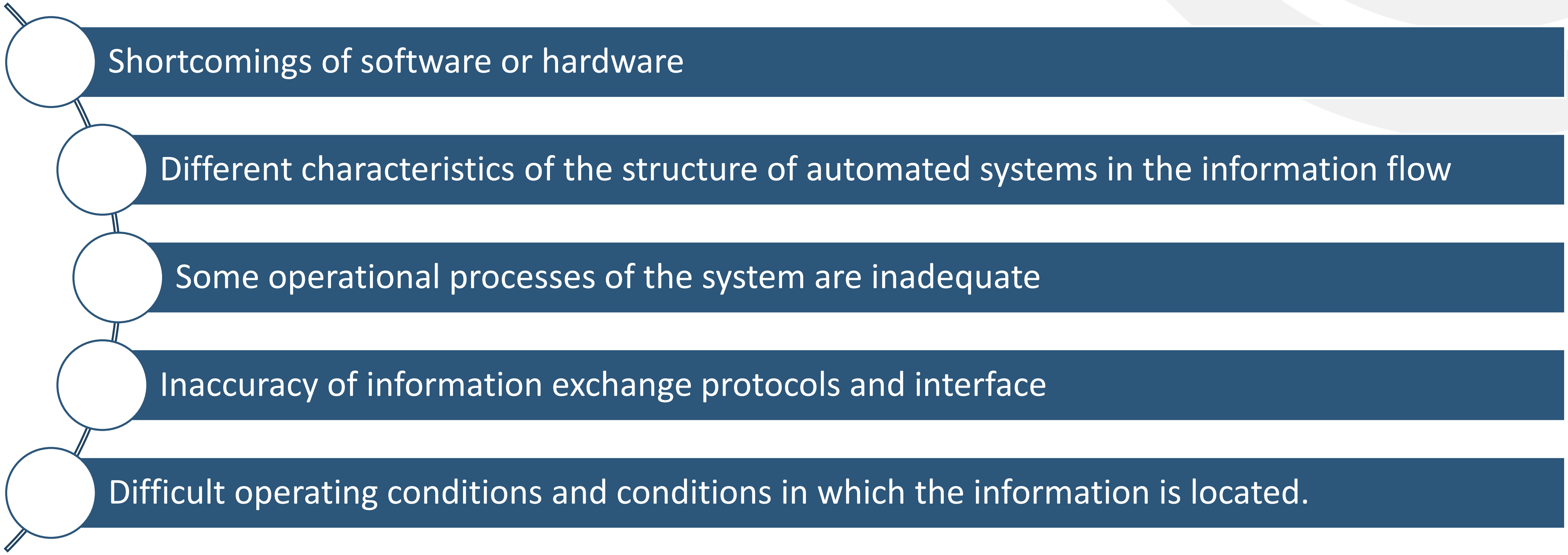
Vulnerabilities

- It refers to being open to attacks or damage which might come internally & externally
- Flaw or weakness within the system
- Can be identified and corrected

VULNERABILITIES

Information security threats are through possible contact with the gaps in the protection system, or factors of vulnerability.

The main vulnerabilities are caused by the following factors:

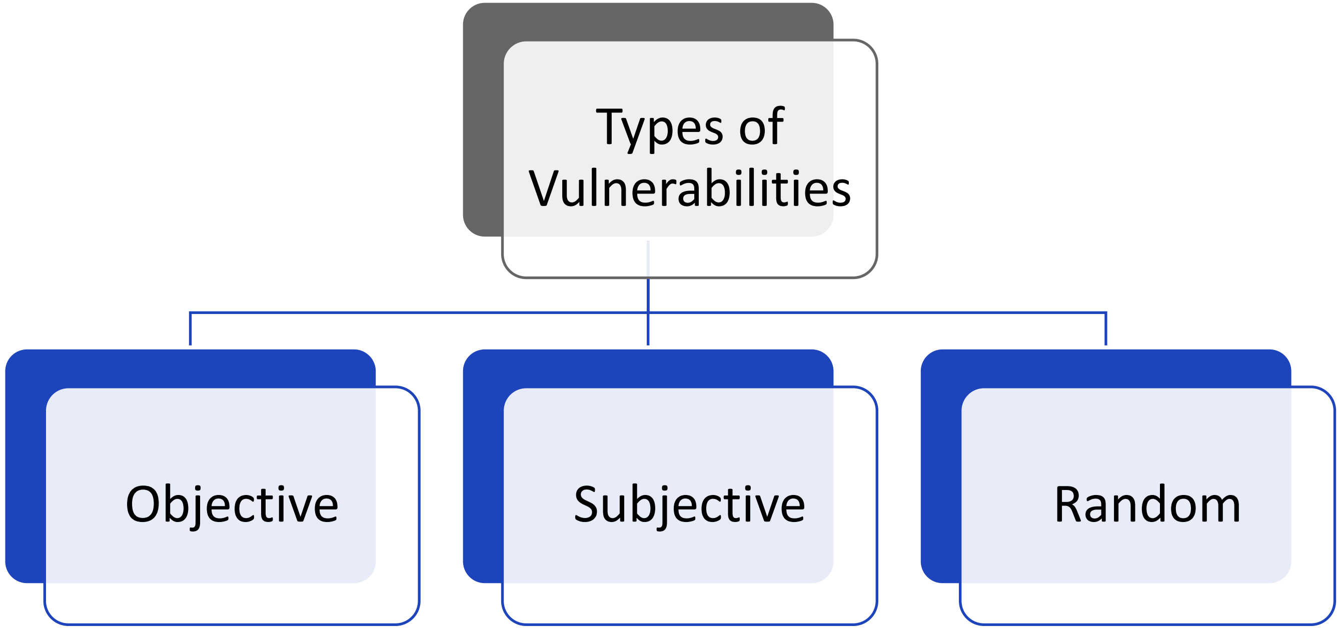


- Shortcomings of software or hardware
- Different characteristics of the structure of automated systems in the information flow
- Some operational processes of the system are inadequate
- Inaccuracy of information exchange protocols and interface
- Difficult operating conditions and conditions in which the information is located.

CLASSIFICATION OF SECURITY VULNERABILITIES

Most often the sources of threats are triggered in order to obtain illegal benefits after damaging information. However, accidental effect of threats due to insufficient protection and mass attack of a threatening factor is also possible.

If you eliminate or at least mitigate the impact from vulnerabilities, you can avoid a significant threat meant to damage the storage system.



Types of Vulnerabilities

Objective

Subjective

Random

Objective vulnerabilities

They depend on the technical design of the equipment which is installed on the object requiring protection, as well as its characteristics. It is impossible to escape all these factors, but their partial elimination can be achieved through engineering techniques in the following cases:

1. Related to emission technical means:
•Electromagnetic techniques (side emission and signals from cable lines, elements of technical means).
•Sound versions (acoustic or with vibration signals).
•Electrical (slip of signals into the circuits of electrical network, through the induction into the lines and conductors, because of uneven current distribution).

2. Activated:
•Malware, illegal programs, technological exits from programs which are together called 'implant tools'.
•Hardware implants: introduced directly into telephone lines, electrical networks or premises.

3. Due to the characteristics of a protected object:
•Object location (visibility and absence of a controlled zone around the information object, presence of vibration or sound reflecting elements around the object, presence of remote elements of the object).
•Arrangement of information exchange channels (use of radio channels, lease of frequencies or use of shared networks).

4. Those that depend on the characteristics of carriers:
•Parts with electro-acoustic modifications (transformers, telephone devices, microphones and loudspeakers, inductors).
•Elements under the influence of electromagnetic field (carriers, microcircuits and other elements).

Subjective vulnerabilities

In most cases, the vulnerabilities of this subtype result from inadequate employee actions at the level of storage and protection system development. Eliminating such factors is possible using hardware and software:

1. Inaccuracies and gross errors that violate information security:

•At the stage of loading the ready software or preliminary algorithm development, as well as during its use (possibly, during daily use or during data entry).

•When managing programs and information systems (difficulties in the training to work with the system, individual set up of services, manipulation of information flows).

•During the use of technical equipment (during switch-on or switch-off, the use of devices for transmitting or receiving information).

2. System malfunctions in the information environment:

•The mode of protection of personal data (the problem may be caused by laid-off employees or current employees during off-hours when they get unauthorized access to the system).

•Safety and security mode (when accessing facilities or technical devices).

•While working with devices (inefficient energy use or improper equipment maintenance).

•While working with data (change of information, its saving, search and destruction of data, elimination of defects and inaccuracies).

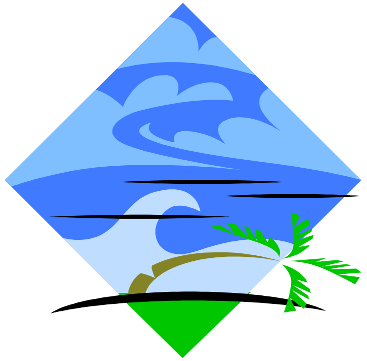
Random vulnerabilities

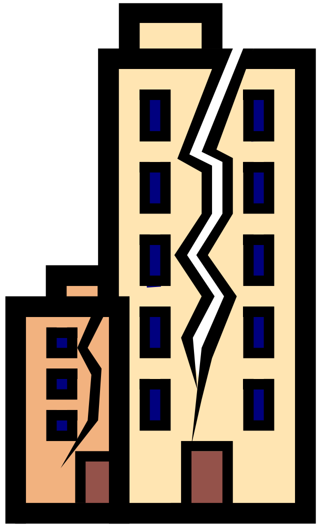
These factors vary depending on unforeseen circumstances and features of the information environment. They are almost impossible to predict in the information space, but you must be prepared to rapidly eliminate them.

Engineering and technical investigation or a response attack will help to mitigate the following problems:

1. System failures:
•Caused by malfunctions of technical means at different levels of processing and storage of information (including those responsible for system performance and access to it).
•Malfunctions and obsolete elements (demagnetization of data carriers, such as diskettes, cables, connection lines and microchips).
•Malfunctions of different software that supports all links in the chain of information storage and processing (antiviruses, application and service programs).
•Malfunctions of auxiliary equipment of information systems (power transmission failures).

2. Factors weakening information security:
•Damage to communications such as water supply, electricity, ventilation and sewerage.
•Malfunctions of enclosing devices (fences, walls in buildings, housing of the equipment where information is stored).





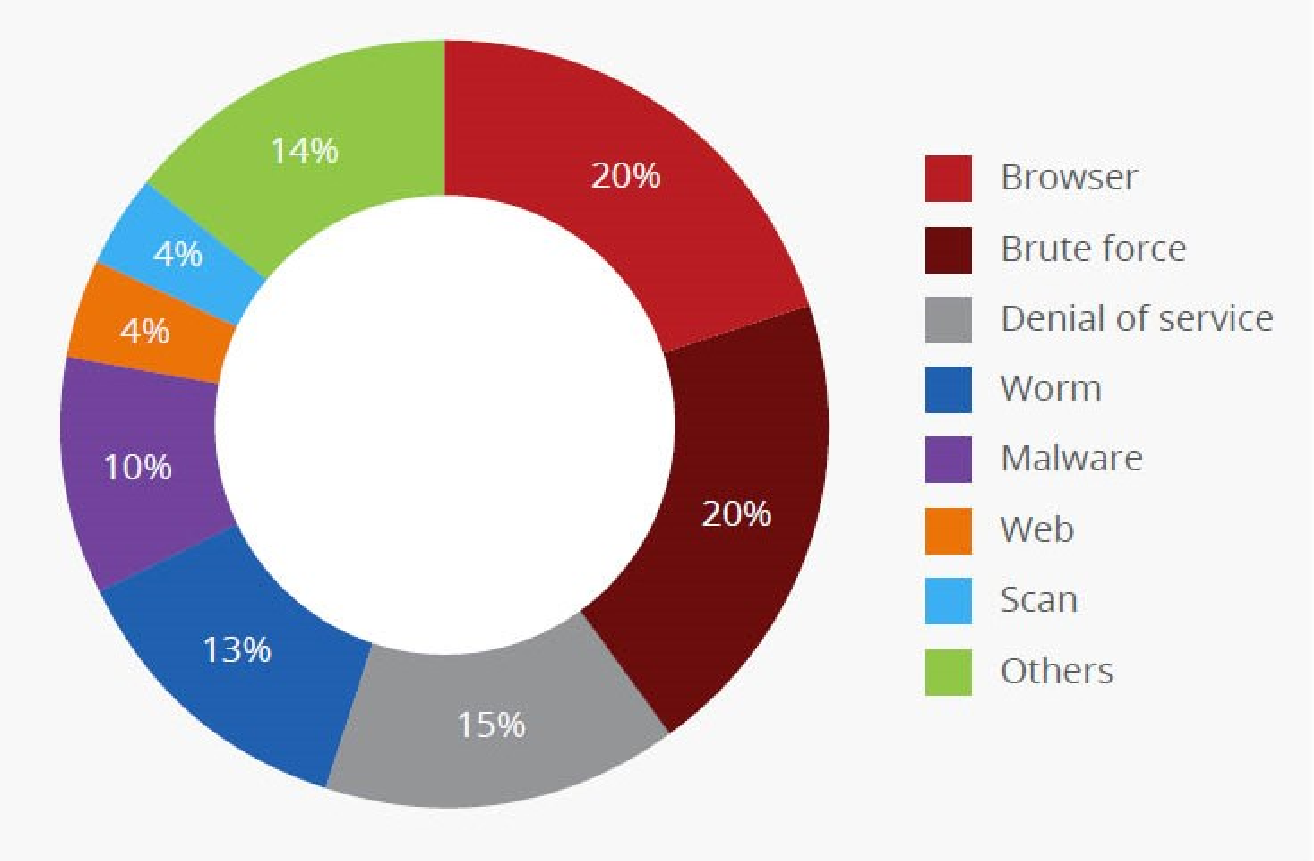
THREATS TO NETWORK SECURITY

- To make sound decisions about security, create policies, and enforce them, management must be informed of the various kinds of threats facing the organization, its applications, data and information systems.
- A **threat** is an object, person, or other entity that represents a constant danger to an asset.
- To better understand the numerous threats facing the organization, a categorization scheme has been developed allowing us to group threats by their respective activities.
- By examining each threat category in turn, management can most effectively protect its information through policy, education and training, and technology controls.

NETWORK SECURITY ATTACKS

Refer to the document: **Malware History**

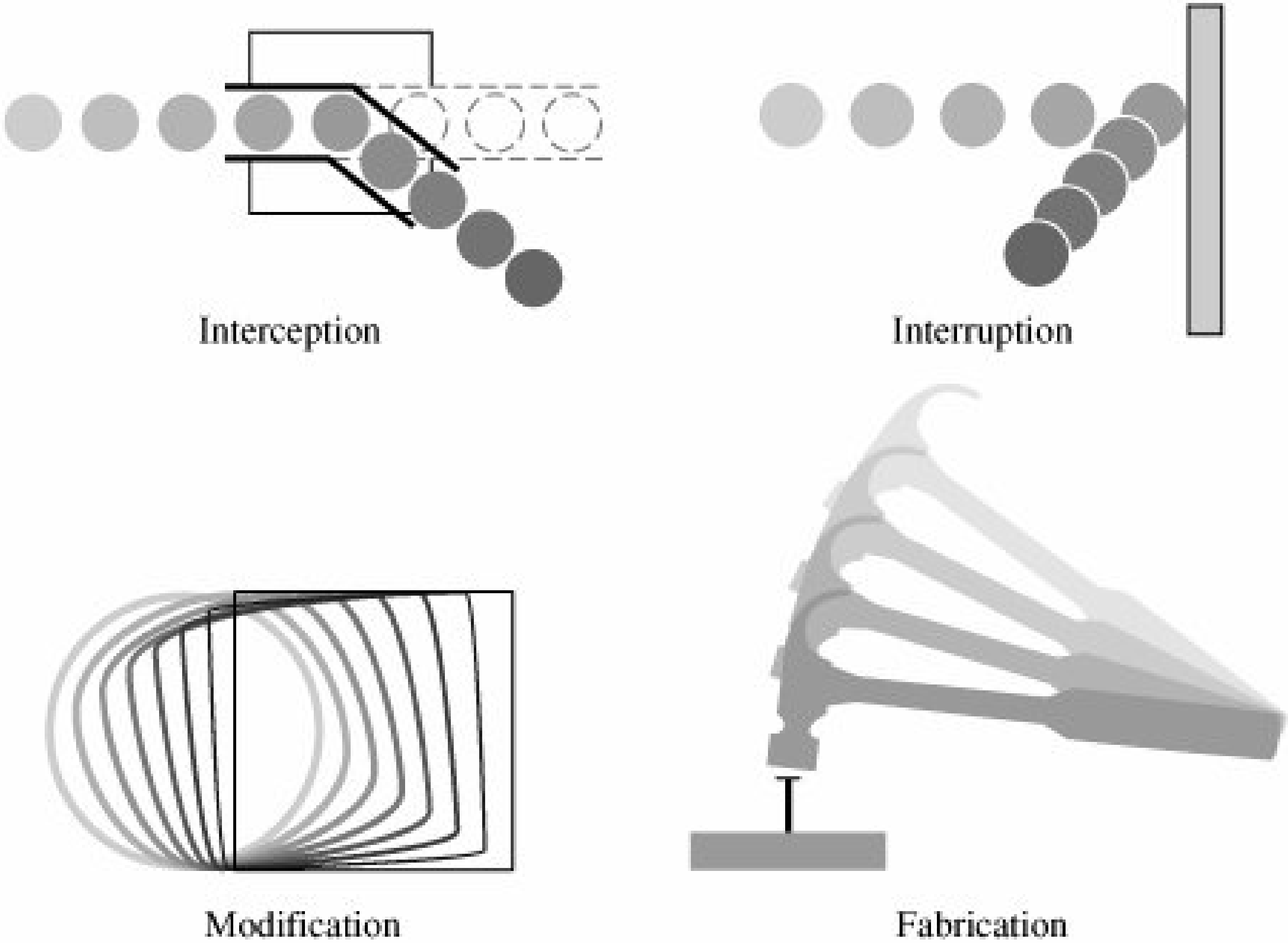
(shared in the Teams)



Source: McAfee Labs, 2017.

TYPES OF NETWORK SECURITY ATTACKS

- Malware
- Interception
- Interruption
- Modification
- Fabrication



TYPES OF MALWARE

Malware is an umbrella term that covers multiple security threats. Infectious malware is comprised of viruses and worms, while Trojans, backdoors and rootkits are concealed pieces of malicious code. Last, but not least, malware for profit gathers spyware, botnets, keystroke loggers, as well as telephony dialers.

- Virus
- Worms & mass mailers
- Trojan Horses
  - Remote access trojan
  - Data destruction trojan
  - Downloader trojan
  - Security Software Disabler
  - DoS & DDoS trojan
  - Dialers
  - Key-loggers

- Backdoors
- Exploits
- Rootkit
- Spyware
- Adware
- Phishing
- Botnet

Refer to the document “Malware History” shared on the Teams

- An **interception** means that some unauthorized party has gained access to an asset. The outside party can be a person, a program, or a computing system. Examples of this type of failure are illicit copying of program or data files, or wiretapping to obtain data in a network. Although a loss may be discovered fairly quickly, a silent interceptor may leave no traces by which the interception can be readily detected.

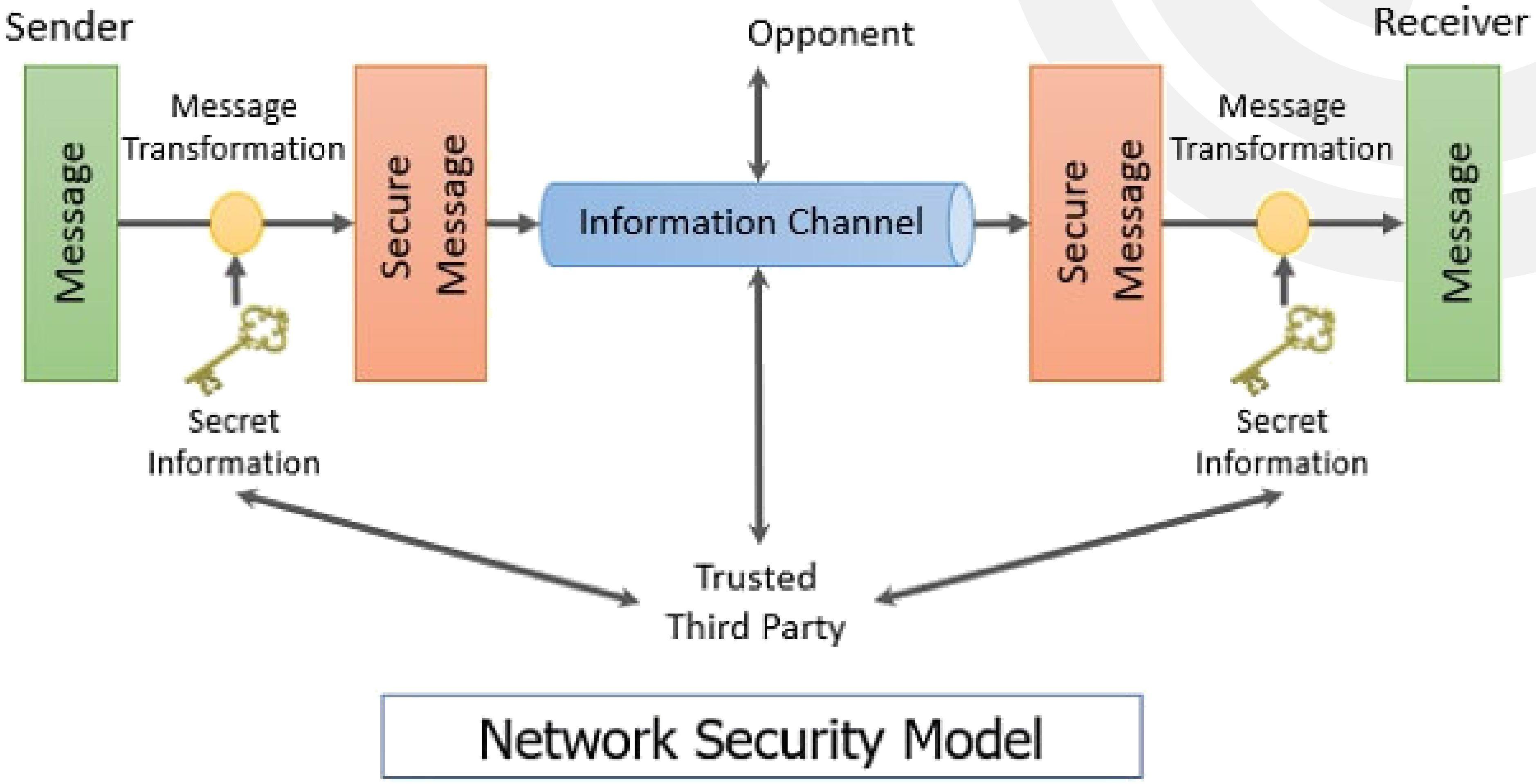
- In an **interruption**, an asset of the system becomes lost, unavailable, or unusable. An example is malicious destruction of a hardware device, erasure of a program or data file, or malfunction of an operating system file manager so that it cannot find a particular disk file.

- If an unauthorized party not only accesses but tampers with an asset, the threat is a **modification**. For example, someone might change the values in a database, alter a program so that it performs an additional computation, or modify data being transmitted electronically. It is even possible to modify hardware. Some cases of modification can be detected with simple measures, but other, more subtle, changes may be almost impossible to detect.

- Finally, an unauthorized party might create a **fabrication** of counterfeit objects on a computing system. The intruder may insert spurious transactions to a network communication system or add records to an existing database. Sometimes these additions can be detected as forgeries, but if skillfully done, they are virtually indistinguishable from the real thing.

Refer to the document "Security Computing" shared on the Teams

MODEL FOR NETWORK SECURITY



Important TTP services for electronic commerce include certification, time-stamping and notarization.