Security rests on confidentiality, integrity and availability.

Interpretation of these aspects and contexts in which they arise vary .

Confidentiality – concealment of information or resources.

Access control mechanisms like cryptography support confidentiality.

It transforms data, makes it incomprehensible.

Other system dependent mechanisms also prevent information from being illicitly accessed.

Confidentiality also applies to existence of data, sometimes more revealing than data itself.

Number of people who distrust politician less important than knowing such a poll taken.

Resource hiding an aspect – organizations want to hide their network configuration, systems they are using.

Integrity

Refers to trustworthiness of data or resources, usually in terms of preventing improper or unauthorized change.

Includes data integrity (content of information) and origin integrity (source of data)

Source of information may bear on its accuracy and credibility and on trust people place in the information.

Integrity mechanisms –2 types - prevention and detection mechanisms

Prevention mechanisms – maintain integrity by blocking unauthorised attempts to change data or attempts to change data in unauthorised ways.

Detection mechanisms simply report data’s integrity no longer trustworthy.

The origin of data, how well it was protected before arriving on current machine and how it is protected on current machine all affect integrity of data.

Integrity includes both correctness and trustworthiness of data.

Availability

Ability to use information or resources.

Denial of service attack – attempts to block availability.

Threat

Potential violation of security. Need not actually occur for there to be a threat.

Confidentiality ,Integrity and Availability counter threats to security of system.

Threats – 4 classes

Disclosure – unauthorized access to information

Deception –Acceptance of false data

Disruption – Interruption or prevention of correct operation

Usurpation - unauthorized control of system

1)Snooping or eavesdropping – unauthorized interception of information

a form of disclosure.

Passive ,some entity is listening to communications or browsing through files and system information.

Passive wiretapping – form of snooping in which a network is monitored.

Confidentiality services seek to counter this threat

2)Modification – an unauthorized change of information covers 3 classes of threats

Goal may be deception in which some entity relies on modified data to determine which action may take, or incorrect information may be accepted as correct and is released.

If modified data controls operation of system, threats of disruption and usurpation arise.

Modification is active - results from an entity changing information unlike snooping.

Active wiretapping – form of modification data moving across a network is altered.

3)Masquerading or spoofing

Impersonation of one entity by another , is a form of both deception and usurpation.

Lures a victim into believing entity with which it is communicating with is a different entity.

If user tries to login into a computer across internet but instead reaches another computer that claims to be desired one, user has been spoofed.

4)Repudiation of origin

False denial an entity sent or created something is a form of deception.

If vendor cannot prove letter came from customer attack succeeds.

5)Denial of receipt

A false denial an entity received some information or message is form of deception.

Customer has already received product ,asking when he will get it.

Denial of service

Attacker prevents server from offering a service.

Policy -statement of what is and what is not allowed.

Security mechanism – method, tool or procedure for enforcing a security policy.