Snooping – unauthorized interception of information , is a form of disclosure

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

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.

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

Active wiretapping – data moving across a network is altered ,new data injected or data is altered.

Active distinguishes it from snooping.

Man in the middle attack – intruder reads messages from sender and sends modified versions to the

Recipient , in hopes recipient and sender won’t realize presence of intermediary.

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.

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

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