INTRODUCTION TO NETWORK SECURITY

Information: is defined as ―knowledge obtained from investigation, Study or Instruction, Intelligence, news, facts, data, a Signature or Character representing data".

Security: is defined as ―freedom from Danger", or Safety: ―Freedom from Fear or Anxiety".

Information Security: "Measures adopted to prevent the unauthorized use, misuse, modification, Denial of use of knowledge, Facts, data or Capabilities**".**
From the above definition, Information Security does guarantees protection.

Computer security: With the introduction of the computer, the need for automated tools for protecting files and other information stored on the computer became evident. This is especially the case for a shared system, and the need is even more acute for systems that can be accessed over a public telephone network, data network, or the Internet. The generic name for the collection of tools designed to protect data and to thwart hackers is **computer security.**

Internet security: Security is affected with the introduction of distributed systems and the use of networks and communications for carrying data between terminal user and computer and between computer and computer. Network security measures are needed to protect data during their transmission. In fact, the term **network security** is somewhat misleading, because virtually all business, government, and academic organizations interconnect their data processing equipment with a collection of interconnected networks. Such a collection is often referred to as an internet, and the term **internet security** is used.

There are no clear boundaries between the above said forms of security.

5.1 The OSI Security Architecture:

The International Telecommunication Union (ITU) Telecommunication Standardization Sector (ITU-T) Recommends X.800, *Security Architecture for OSI*, defines a systematic

approach. The OSI security architecture provides overview of many of the concepts and it focuses on security attacks, mechanisms, and services.

Security attack: Any action that compromises the security of information owned by an organization.

Security mechanism: A process (or a device incorporating such a process) that is designed to detect, prevent, or recover from a security attack.

Security service: A processing or communication service that enhances the security of the data processing systems and the information transfers of an organization. The services are intended to counter security attacks, and they make use of one or more security mechanisms to provide the service.

The terms *threat* and *attack* are commonly used to mean more or less the same thing and the actual definitions are

Threat: A potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm. That is, a threat is a possible danger that might exploit vulnerability.

Attack: An assault on system security that derives from an intelligent threat; that is, an intelligent act that is a deliberate attempt (especially in the sense of a method or technique) to evade security services and violate the security policy of a system.

5.2 Security Attacks:

Security attacks, used both in X.800 and RFC 2828, are classified as pas*sive attacks* and *active attacks*.

A passive attack attempts to learn or make use of information from the system but does not affect system resources.

An active attack attempts to alter system resources or affect their operation.