UNIT I
Introduction: Basic Terminology

GALGOTIAS
UNIVERSITY

Network Security

Network security is any activity designed to protect the usability and integrity of your network and data.

- ❑ It includes both hardware and software technologies
- ❑ It targets a variety of threats
- ❑ It stops them from entering or spreading on your network
- ❑ Effective network security manages access to the network

Network Security Goals

The network security can be considered through the achievement of **two main security goals**:

Computer system security :- is to protect information assets against unauthorized or malicious use as well as to protect the information stored in computer systems from unauthorized disclosure, modification or destruction

Communication security:- is to protect information during its transmission through a communication medium from unauthorized.

Network security Services

❑ Sharing resources and communication requires two
   components:-
   server component that provides access to the resource
   client component that requests access to the resource

Both components are referred to as a service
❑ NOSs must be outfitted with the types of services your
   client operating systems require, whether they are Web
   servers, e-mail servers, file and print servers.

SECURITY SERVICES

The security objectives are accomplished through security policies and security services. A security policy is the set of criteria that define the provision of security services, where a security service is a service which is provided by a layer of communicating open systems, in order to ensure adequate security of the systems or of data transfers.

✓Network security services is a set of libraries designed to support cross-platform development of security-enabled client and server applications.

✓A set of libraries designed to support cross-platform development of security-enabled client and server applications with optional support for hardware TLS/SSL acceleration on the server side and hardware smart cards on the client side
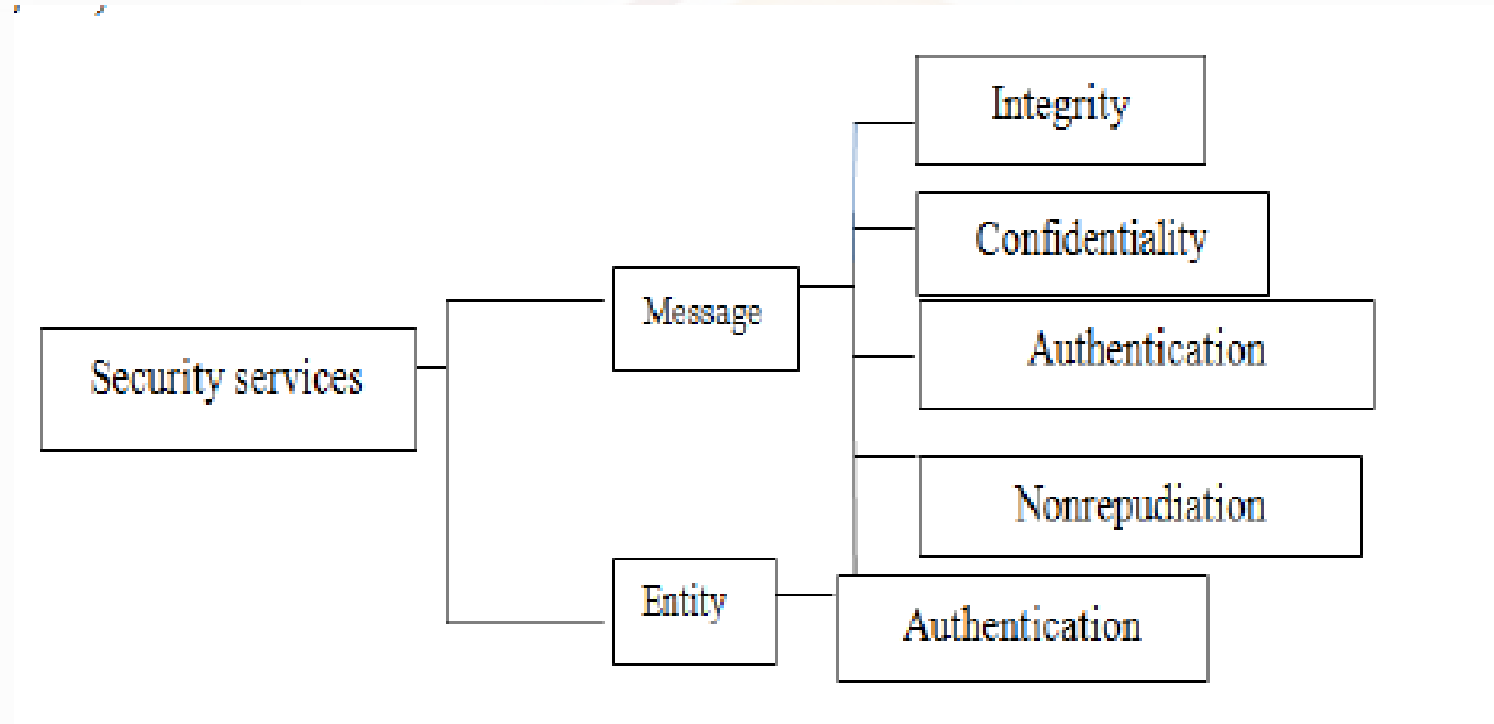
Network security services

Authentication

Authentication is the process of recognizing a user's identity. It is the mechanism of associating an incoming request with a set of identifying credentials. The credentials provided are compared to those on a file in a database of the authorized user's information on a local operating system or within an authentication server.

❑ Password authentication
❑ Two-factor authentication
❑ Token authentication
❑ Biometric authentication
❑ Transaction authentication
❑ Computer recognition authentication
❑ CAPTCHAs
❑ Single sign-on

Access Control

Network access control is a method of enhancing the security of a private organizational network by restricting the availability of network resources to endpoint devices that comply with the organization's security policy.

Access control scheme comprises of two major components

✓**Restricted Access to the network devices**
✓**Network Boundary Protection**

Data Confidentiality

Protecting information from being accessed by unauthorized parties.

- ✓ Connection
- ✓ Connectionless
- ✓ Selective- field Confidentiality
- ✓ Traffic flow Confidentiality

Ensures that during their transmission the data is not altered by unauthorized principles.

- ❏ Connection integrity with recovery
- ❏ Connection integrity without recovery
- ❏ Selective field connection integrity
- ❏ Connectionless integrity
- ❏ Selective field connectionless integrity

Nonrepudiation

Protection against denial of sending or receiving in the communication.

Two forms are :-

Non-repudiation(origin)
Non-repudiation (destination)

SECURITY MECHANISMS

- ❑ Encipherment mechanisms
- ❑ Digital Signatures
- ❑ Access Control mechanisms
- ❑ Traffic-padding mechanisms
- ❑ Routing Control mechanisms
- ❑ Notarization mechanisms

Thank You