Chapter one

Introduction to Computer Network and Information Security

COMPUTER SECURITY

- **Computer security** is about provisions and policies adopted to protect information and property from theft, corruption, or natural disaster while allowing the information and property to remain accessible and productive to its intended users.
- **Computer Network :** the interconnection of computers
- **Security:** is the protection afforded to an *automated information* system in order to attain the applicable objectives of preserve the integrity, availability, and confidentiality of information system resources (includes hardware, software, firmware, information/ data, and telecommunications).
- **Confidentiality: This term covers two related concepts:**
  - **Data confidentiality:** Assures that private or confidential information is not made available or disclosed to unauthorized individuals.
  - **Privacy:** Assures that individuals control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed.

- **Integrity: This term covers two related concepts:**
  - **Data integrity:** Assures that information and programs are changed only in a specified and authorized manner.
  - **System integrity:** Assures that a system performs its intended function in an unimpaired(modifies) manner, free from deliberate or inadvertent unauthorized manipulation of the system.
- **Availability:** Assures that systems work promptly and service is not denied to authorized users.

Additional security concepts:

- **Authenticity:**
  - The property of being genuine and being able to be **verified and trusted**; confidence in the validity of a transmission, a message, or message originator.
  - This means **verifying that users are who they are** and that each input arriving at the system came from a trusted source.
- **Accountability:**
  - The security goal that generates the requirement for actions of an entity to be traced uniquely to that entity.
  - This supports non repudiation, deterrence, fault isolation, intrusion detection and prevention, and after-action recovery and legal action.
  - Because truly secure systems are not yet an achievable goal, we must be able to trace a security breach to a responsible party.
  - Systems must keep records of their ***activities to permit later*** forensic analysis to trace security breaches or to aid in transaction disputes.

Over View of Network Layer

- The topics that we will be discussing would be based on the diagram below.

OSI Layer Name	TCP/IP Layer Name	Encapsulation Units
Application	Application	data
Presentation		data
Session		data
Transport	Transport	segments
Network	Internet	packets
Data Link	Network Access	frames
Physical		bits

The Upper Layers

OSI	TCP / IP
Application (Layer7)	Application
Presentation (Layer6)	
Session (Layer 5)	

- Session
- Presentation
- Application

The Session Layer

The Session layer permits two parties to hold ongoing communications called a session across a network.

- Not found in TCP/IP model
- In TCP/IP,its characteristics are provided by the TCP protocol.

  (Transport Layer)

The Presentation Layer

The Presentation Layer handles data format information for networked communications. This is done by converting data into a generic format that could be understood by both sides.

- Not found in TCP/IP model
- In TCP/IP, this function is provided by the Application Layer.

The Application Layer

The Application Layer is the top layer of the reference model. It provides a set of interfaces for applications to obtain access to networked services as well as access to the kinds of network services that support applications directly.

- OSI - FTAM,VT,MHS,DS,CMIP

  TCP/IP - FTP,SMTP,TELNET,DNS,SNMP

- Although the notion of an application process is common to both, their approaches to constructing application entities is different.

Transport Layer

OSI	TCP / IP
Transport (Layer 4)	**Transport (TCP/UDP)**

- The functionality of the transport layer is to provide “transparent transfer of data from a source end open system to a destination end open system” (ISO / IEC 7498: 1984).

Transport Layer

- Transport is responsible for creating and maintaining the basic end-to-end connection between communicating open systems, ensuring that the bits delivered to the receiver are the same as the bits transmitted by the sender; in the same order and without modification, loss or duplication

OSI Transport Layer

- It takes the information to be sent and breaks it into individual packets that are sent and reassembled into a complete message by the Transport Layer at the receiving node.

- Also provide a signaling service for the remote node so that the sending node is notified when its data is received successfully by the receiving node

OSI Transport Layer

- Transport Layer protocols include the capability to acknowledge the receipt of a packet; if no acknowledgement is received, the Transport Layer protocol can retransmit the packet or time-out the connection and signal an error

OSI Transport Layer

- Transport protocols can also mark packets with sequencing information so that the destination system can properly order the packets if they're received out-of-sequence
- In addition, Transport protocols provide facilities for insuring the integrity of packets and requesting retransmission should the packet become garbled when routed.

OSI Transport Layer

- Transport protocols provide the capability for multiple application processes to access the network by using individual local addresses to determine the destination process for each data stream.

TCP/IP Transport Layer

- Defines two standard transport protocols: TCP and UDP
- TCP implements a reliable data-stream protocol
  - connection oriented.
- UDP implements an unreliable data-stream
  - connectionless

- **Protocol:** An agreement between parties on how communication should take place.
- Protocols define format, order of messages sent and received among network entities, and actions taken on message transmission, receipt
- All communication activity in the Internet are governed by protocols.

TCP/IP Transport Layer

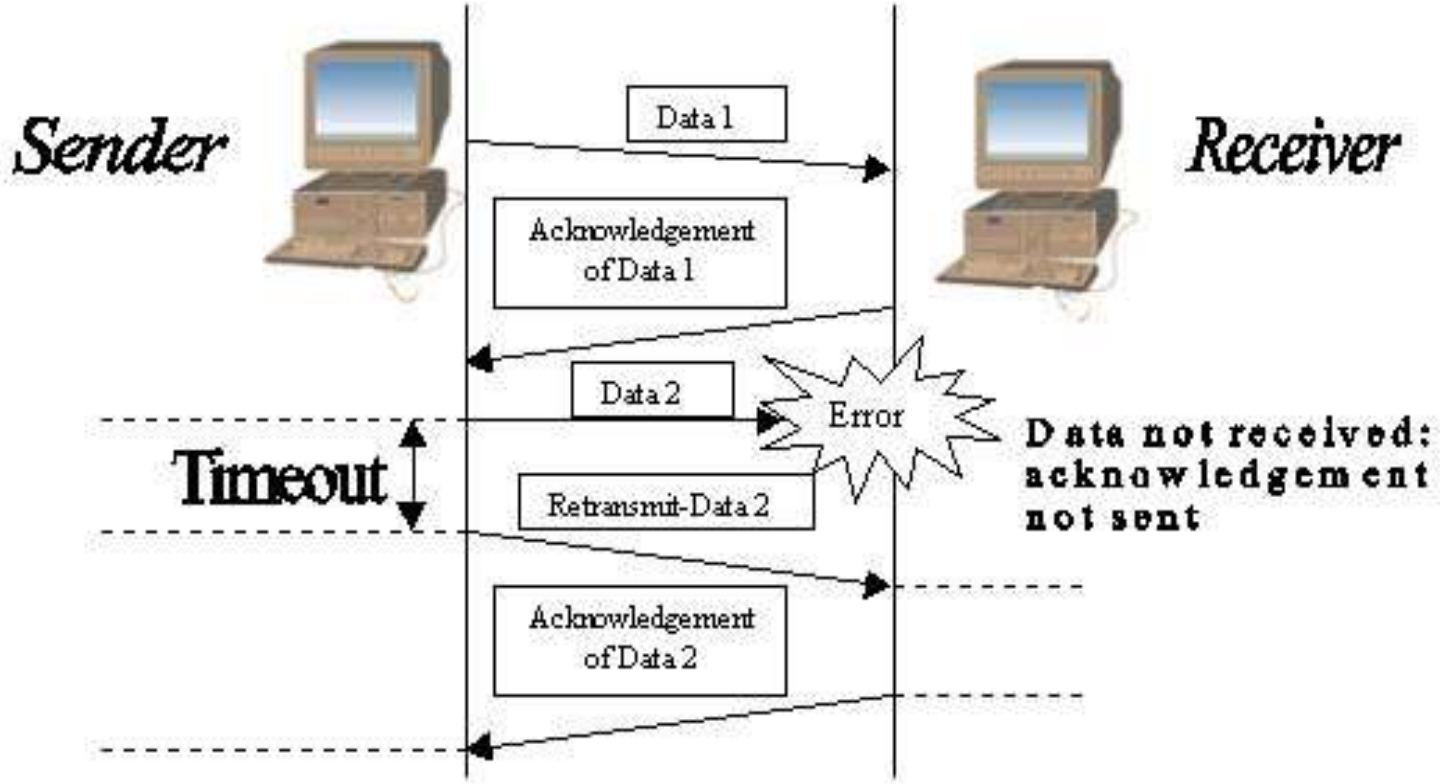
- TCP provides reliable data transmission
- UDP is useful in many applications
  - E.g. Where data needs to be broadcasted or multicast
- Primary difference is that UDP does not necessarily provide reliable data transmission

TCP/IP Transport Layer

- TCP is responsible for data recovery
  - by providing a sequence number with each packet that it sends
- TCP requires ACK (ackowledgement) to ensure correct data is received
- Packet can be retransmitted if error detected

- Use of ACK

TCP/IP Transport Layer



TCP/IP Transport Layer

- TCP and UDP introduce the concept of *ports*
- Common ports and the services that run on them:
  - FTP 21 and 20
  - telnet 23
  - SMTP 25
  - http 80
  - POP3 110

TCP/IP Transport Layer

- By specifying ports and including port numbers with TCP/UDP data, *multiplexing* is achieved
- Multiplexing allows multiple network connections to take place simultaneously
- The port numbers, along with the source and destination addresses for the data, determine a *socket*

Network vs. Internet

OSI	TCP / IP
Network (Layer 3)	**Internet**

- Like all the other OSI Layers, the network layer provides both connectionless and connection-oriented services. As for the TCP/IP architecture, the internet layer is exclusively connectionless.

Network vs. Internet

- OSI Routing Architecture
  - End systems (ESs) and intermediate systems (ISs) use routing protocols to distribute ("advertise") some or all of the information stored in their locally maintained routing information base. ESs and ISs send and receive these routing updates and use the information that they contain (and information that may be available from the local environment, such as information entered manually by an operator) to modify their routing information base.

Data link / Physical vs. Network

OSI	TCP / IP
Data Link (Layer 2)	**Network**
Physical (Layer 1)	

- Data link layer
  - The function of the *Data Link Layer* is "provides for the control of the physical layer, and detects and possibly corrects errors which may occur" (IOS/IEC 7498:1984). In another words, the Data Link Layer transforms a stream of raw bits (0s and 1s) from the physical into a data frame and provides an error-free transfer from one node to another, allowing the layers above it to assume virtually error-free transmission

Data link / Physical vs. Network

- Physical layer
  - The function of the *Physical Layer* is to provide "mechanical, electrical, functional, and procedural means to activate a physical connection for bit transmission" (ISO/IEC 7498:1984). Basically, this means that the typical role of the physical layer is to transform bits in a computer system into electromagnetic (or equivalent) signals for a particular transmission medium (wire, fiber, ether, etc.)

- The **Physical Layer** describes the physical properties of the various communications media, as well as the electrical properties and interpretation of the exchanged signals.
  - Ex: this layer defines the size of Ethernet coaxial cable, the type of BNC connector used, and the termination method.

- The **Data Link Layer** describes the logical organization of data bits transmitted on a particular medium.
  - Ex: this layer defines the framing, addressing and check summing of Ethernet packets.