Keamanan Sistem Komputer

Network Concepts, Threat

Network Concepts

- Network Transmission Media
- Protocol Layers
- Addressing and Routing

Network Transmission Media

- Data being transmitted can be intercepted (eavesdrop, wiretap, or sniff)
- Both transmitting data on either wire or wireless are vulnerable.

Network Transmission Media

- Cable

  The most local level, all signals in an Ethernet or other LAN are available in the cable for everyone to intercept.

- Packet Sniffing

  A device called packet sniffer retrieves all packets on its LAN.

- Radiation

  Ordinary wire emits radiation, and by process called inductance an intruder can tap a wire and read radiated signals without making physical contact with the cable.

Network Transmission Media

- Optical Fiber

  Offers two significant security advantages: the entire optical network must be tuned carefully each time a new connection is made so no one can tap the system without detection; it carries light energy so inductive tap is impossible.

- Microwave

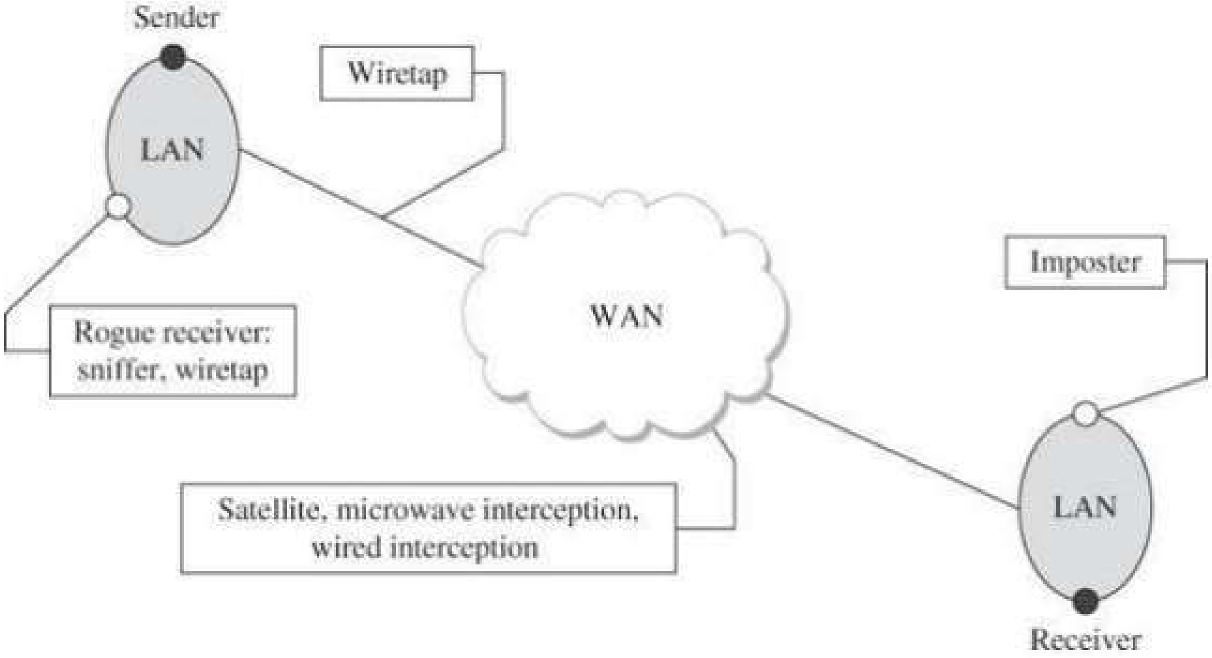
  Broadcasted though the air, more accessible to outsiders.

- Satellite Communication

  The potential of interception is bigger than microwave signals, however because satellite communications are geneally heavily multiplexed, the risk of interception is small.

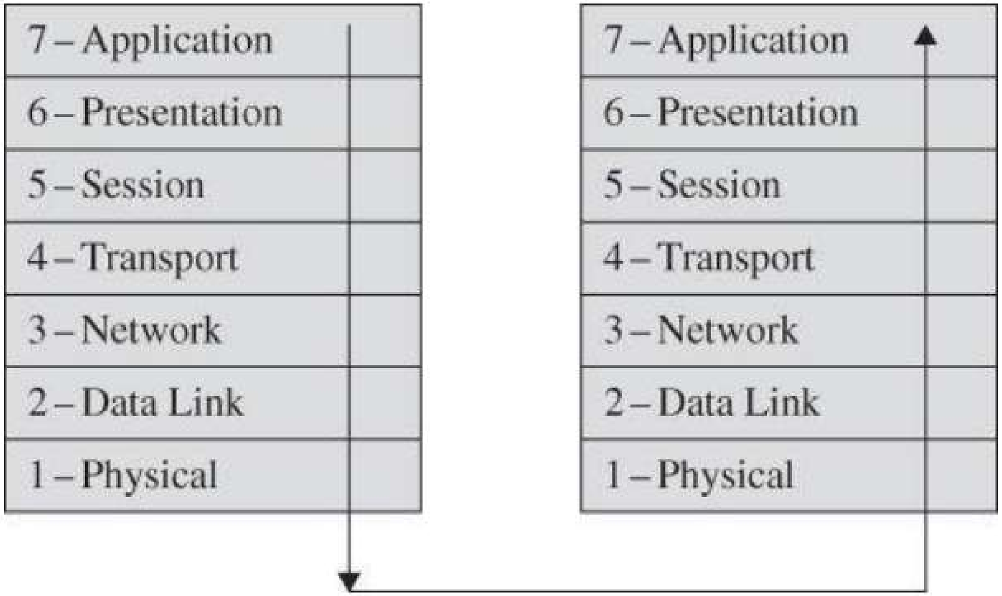
Network Transmission Media (Summary)

- Network traffic is available to an inceptor at many points.
- All network communications are potentially exposed to interception; sensitive signals must be protected.



Protocol Layers

- Network communications are performed through a virtual concept called the OSI model.

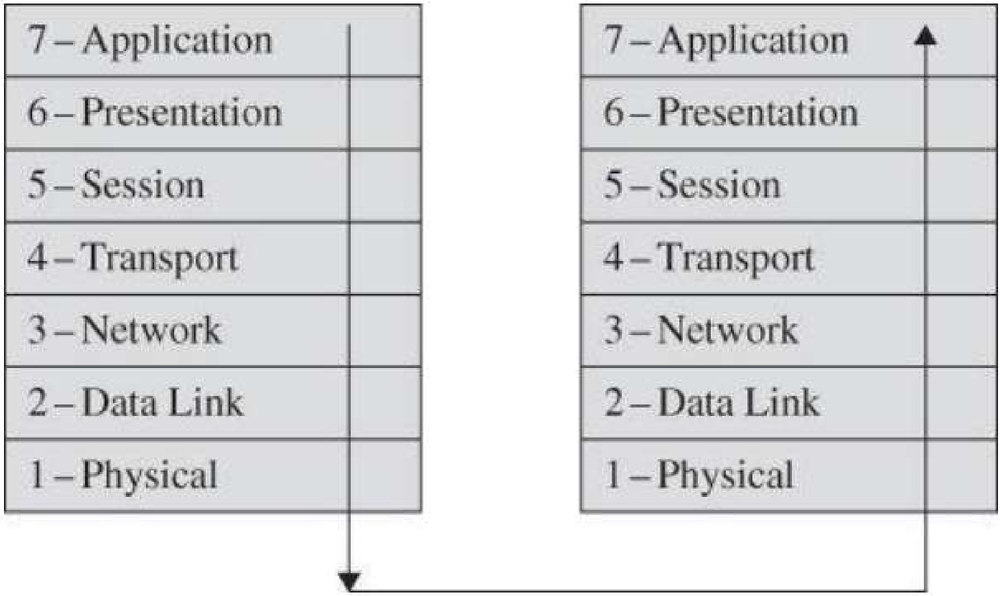


7 – Application
6 – Presentation
5 – Session
4 – Transport
3 – Network
2 – Data Link
1 – Physical

7 – Application
6 – Presentation
5 – Session
4 – Transport
3 – Network
2 – Data Link
1 – Physical

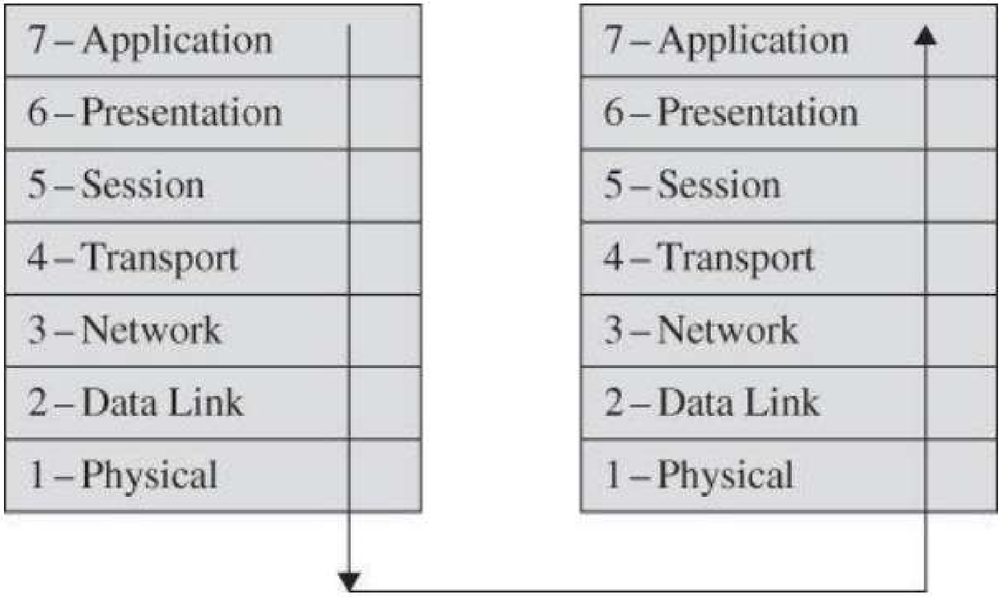
Protocol Layers

- Application prepares data to be transmitted through a network. Data move down through the layers, being transformed and repackaged. Control information is added in headers and footers. Finally, data are ready to travel on a physical medium



Protocol Layers

- On the receiving end, data enter the bottom of the model and progress up through the layers where control information is examined and removed, and data are reformatted. Finally, data arrive at an application at the top layer of the model for the receiver.



Protocol Layers (Summary)

- Interception can occur at any level of this model:
  - The application can covertly leak data
  - The physical media can be wiretapped
  - Session between two subnetworks can be compromised

Addressing and Routing

Protocols

- The communication is separated from the actual medium of communication.
- It is possible because there is a defined protocols.
- The details of how the communication is accomplished are hidden within software and hardware at both ends.
- The software and hardware enable users to implement a network according to a protocol stack.

Addressing and Routing

Addressing

- At the network layer, a hardware device called a router actually sends the message from your network to a router on the network of the destination host.
- Network layer adds two header to show user's computer address as the source and the destination's address as the destination.

Addressing and Routing

Routing

- Using routers to redirect packets to get them closer to their destination.

Ports

- Number associated with an application program that serves or monitors for a network service.

War on Networks: Network Security Attacks

Threats to network communications:

- Interception (eavesdropping or wiretapping)
- Modification (integrity failure)
- Fabrication (integrity failure)
- Interruption (denial of service)

Interception: Eavesdropping and Wiretapping

- Even backdoor intended only for court-authorized wiretaps can be misused.
- Interception is a passive threat: communication goes on normally, except that a hidden third party has listened in, too.
- Encryption is the strongest and most commonly used countermeasures against interception.

Interception: Eavesdropping and Wiretapping

What makes a network vulnerable to interception?

- Anonymity

  Attacker can mount an attack from thousands of miles away and never come into direct contact with the system. The attack can be passed through many other hosts to disguise the attack’s origin.

- Many points of attack

  When a file is stored in a network host remote from the user, the data may pass through many hosts to get to the user. An attack can come from any host to any host, so a large network offers many points of vulnerability

Interception: Eavesdropping and Wiretapping

What makes a network vulnerable to interception?

- Sharing

  Networked systems open up potential access to more users than do single computers.

- System Complexity

  The attacker can use victim’s computer to perform part of the attacker computation. Most users have no idea of all the processes active in the background of their computers.

Interception: Eavesdropping and Wiretapping

What makes a network vulnerable to interception?

- Unknown Perimeter

  Network expandability also implies uncertainty about the network boundary. One host may be a node on a two different network, so resources on one network are accessible to the users of the other network as well.

  This is a security disadvantage since unknown or uncontrolled group is a possibly of malicious users.

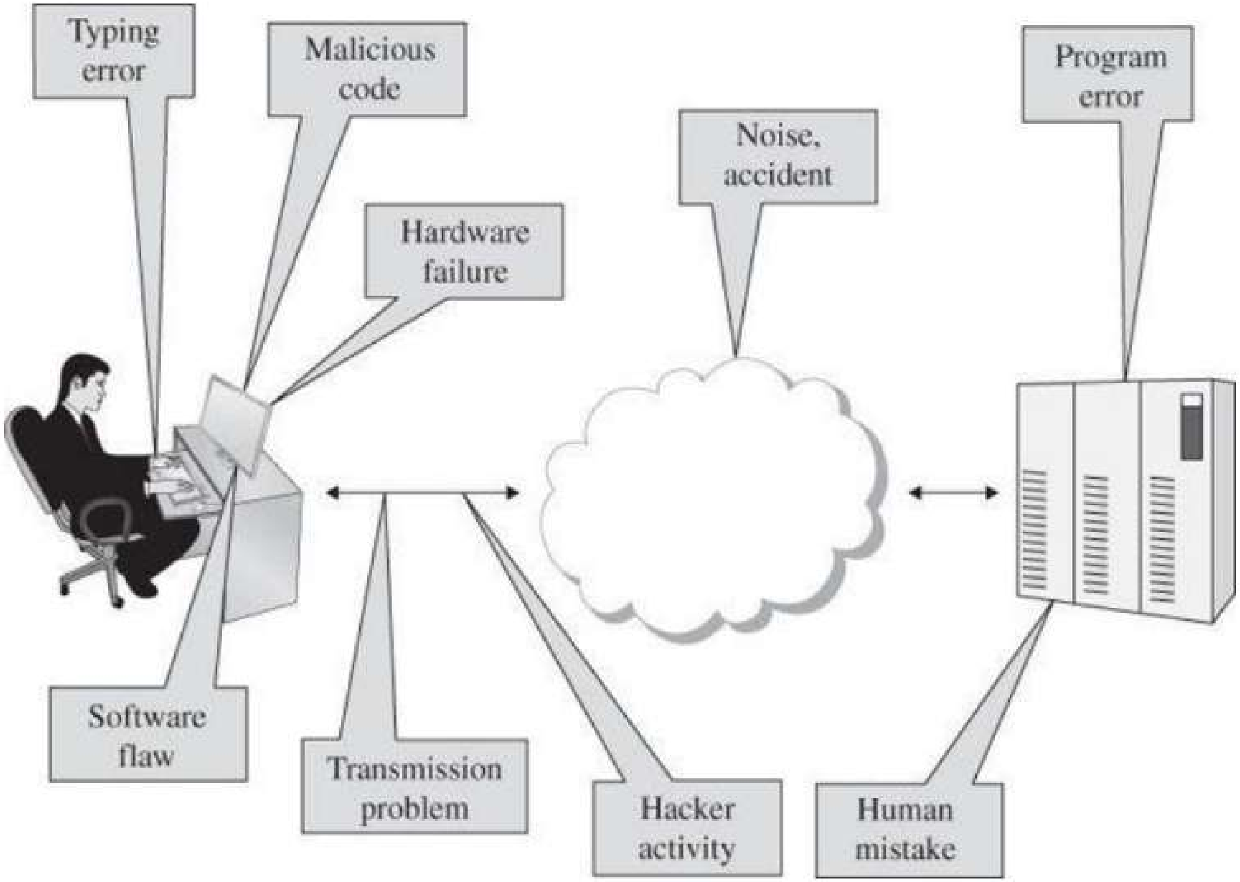
Modification, Fabrication: Data Corruption

The act involves:

- Modifying data en route (modification)
- Crafting new content (insertion)
- Repeating existing communication (replay)

Can occur during data entry, in storage, during use and computation, in transit, and on output and retrieval.

Modification, Fabrication: Data Corruption



Modification, Fabrication: Data Corruption

- Communications media are known to be vulnerable to data corruption.
- Simple factors such as weather and trees can interfere with clean transmission.
- For this reason communication protocols include features to check for and correct, at least some, errors in transmission.

Modification, Fabrication: Data Corruption

Some modification failures:

- Sequencing

  Involves permuting the order of data, occurs when a later fragment of a data stream arrives before a previous one.

- Substitution

  Replacement of one piece of data stream with another. The obvious countermeasure against substitution attacks is encryption, covering the entire message or creating an integrity check.

Modification, Fabrication: Data Corruption

Some modification failures:

- Insertion

  Almost a form of substitution, in which data values are inserted into a stream. Attacker does not even need to break an encryption scheme.

- Replay

  Legitimate data are intercepted and reused, without modification. The classic example of replay attack involves financial transactions: a merchant processes a credit card or funds transfer on behalf of a user and then, seeing that the transfer succeeded, resubmits another transaction.

Interruption: Loss of Service

- Routing

  Routing supports efficient resource use and quality or service. But if misused, it can cause denial of service.

- Excessive Demands

  Network capacity is enormous but finite, and capacity of any particular link or component is much smaller. Denial-of-service attacks usually try to flood a victim with excessive demand.

Interruption: Loss of Service

- Port Scanning

  Being used as the first step in an attack, to determine what further attacks might succeed. Using a port scanner, network information can be easily gathered. A port scan maps the topology and hardware-software components of a network segment.

  Port scanner tells attacker three things: which standard ports or services are running, what OS is installed, and what applications and versions of applications are present. All these inormations can obtained anonymously.

  Network and vulnerability scanners can be used positively for management and administration or negatively for attack planning.

Vulnerability Summary

- Numerous attacks against the infrastructure of wide area networks can lead to interception, modification, and denial of service.
- The attacks work against large network, they are seldom used against one specific user.