CS 547: Foundation of Computer Security

S. Tripathy
IIT Patna

Summary: Security services & mechanisms

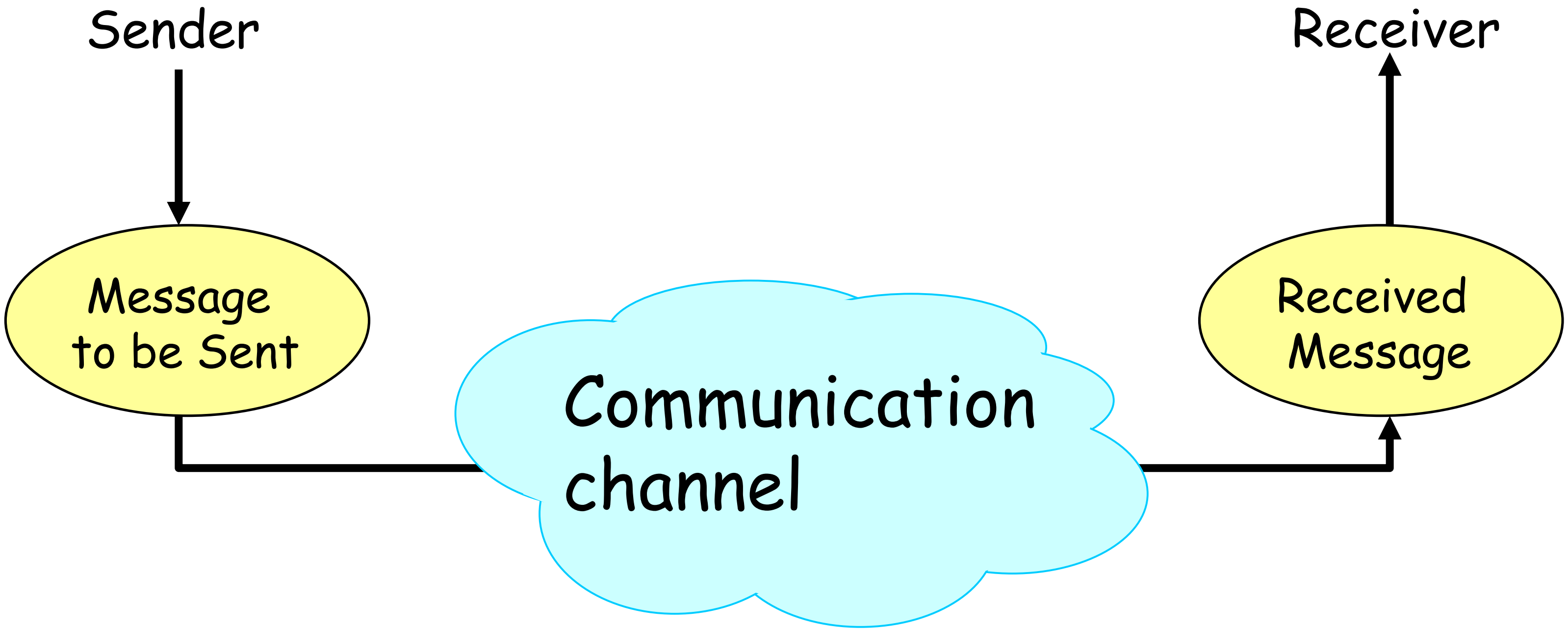
Security Services	Security Mechanisms
Confidentiality	→Encryption
Integrity	→MAC (keyed-hash)
Authentication	→Login
Availability	→Redundancy
Non-repudiation	→Digital Signature
Access Control	→Discretionary/ Mandatory Access control
Accountability	→System Audit

Characteristics of the Internet

- Different types of nodes
  - Server, laptop, router, UNIX, Windows,…
- Different types of communication links
  - Wireless vs. wired

- No single entity that controls the Internet
- Traffic from a source to a destination likely flows through nodes controlled by different, unrelated entities
- End nodes cannot control through which nodes traffic flows
  - Worse, all traffic is split up into individuals packets, and each packet could be routed along a different path

Threats/ Attacks



- Three key points of vulnerability:
  - Sender (Client /Server)
  - Receiver (Server/ Client)
  - Communications channel

What Attacker Can do?

Read communication

Modify communication

Forge communication

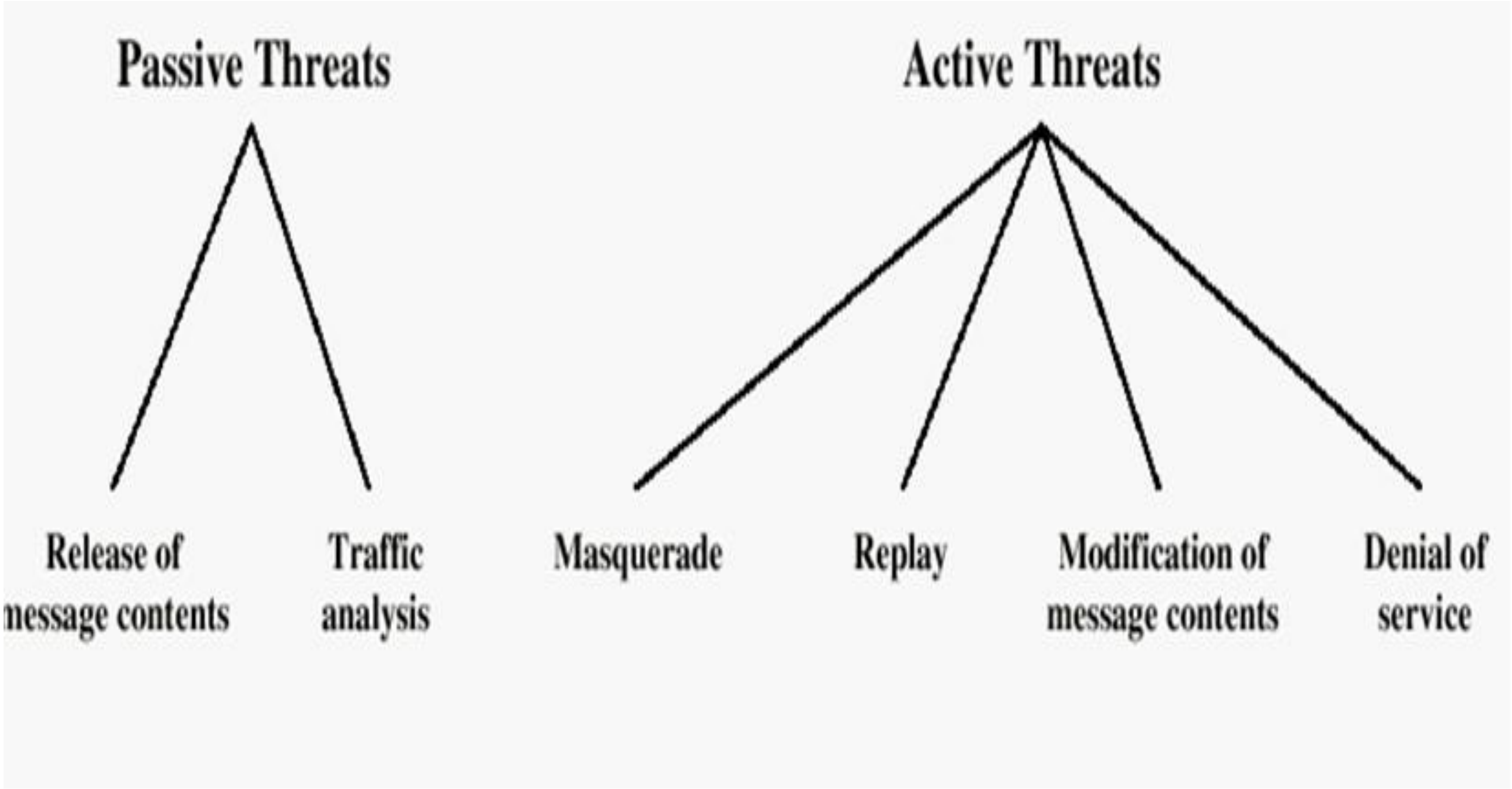
Inhibit communication

Kinds of Threats

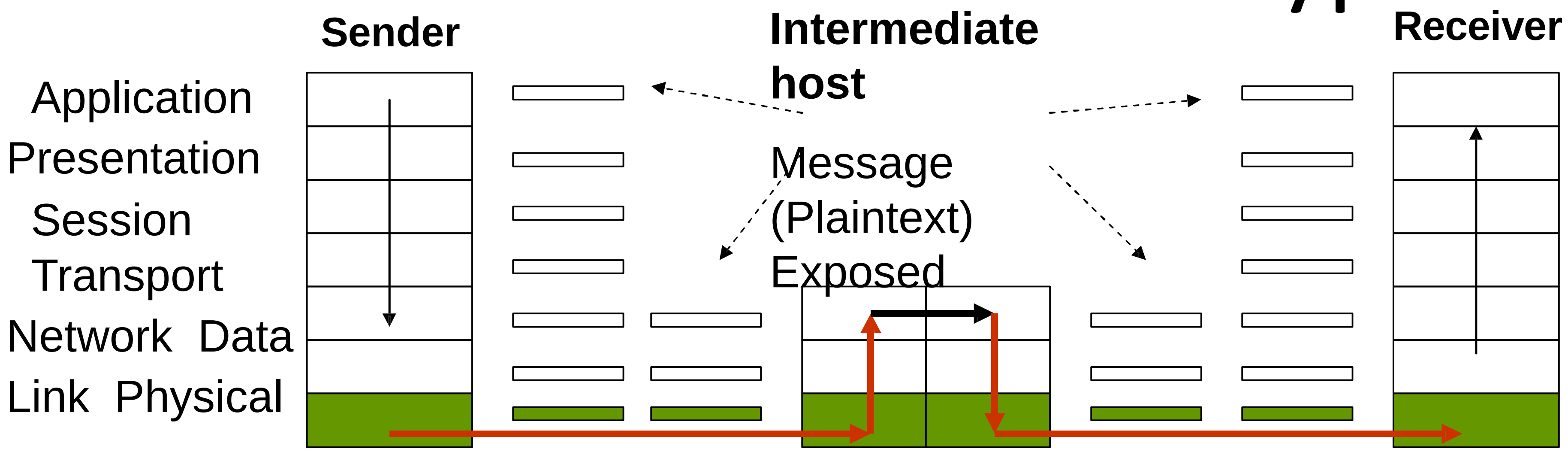
- Intercepting data in traffic
- Modifying data in transit
- Inserting communications
- Impersonating a user
- Inserting a repeat of a previous communication
- Blocking selected traffic
- Blocking all traffic

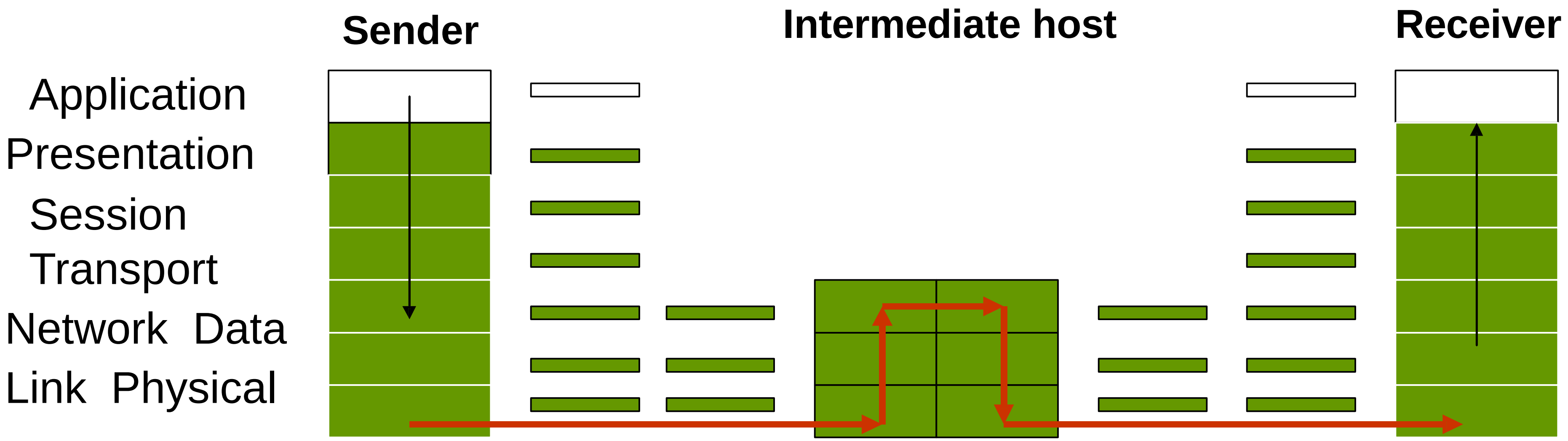
- Accessing programs or data at remote hosts
- Modifying programs or data at remote hosts
- Running a program at a remote host

Passive and Active Threats



Link & End-to-End Encryption



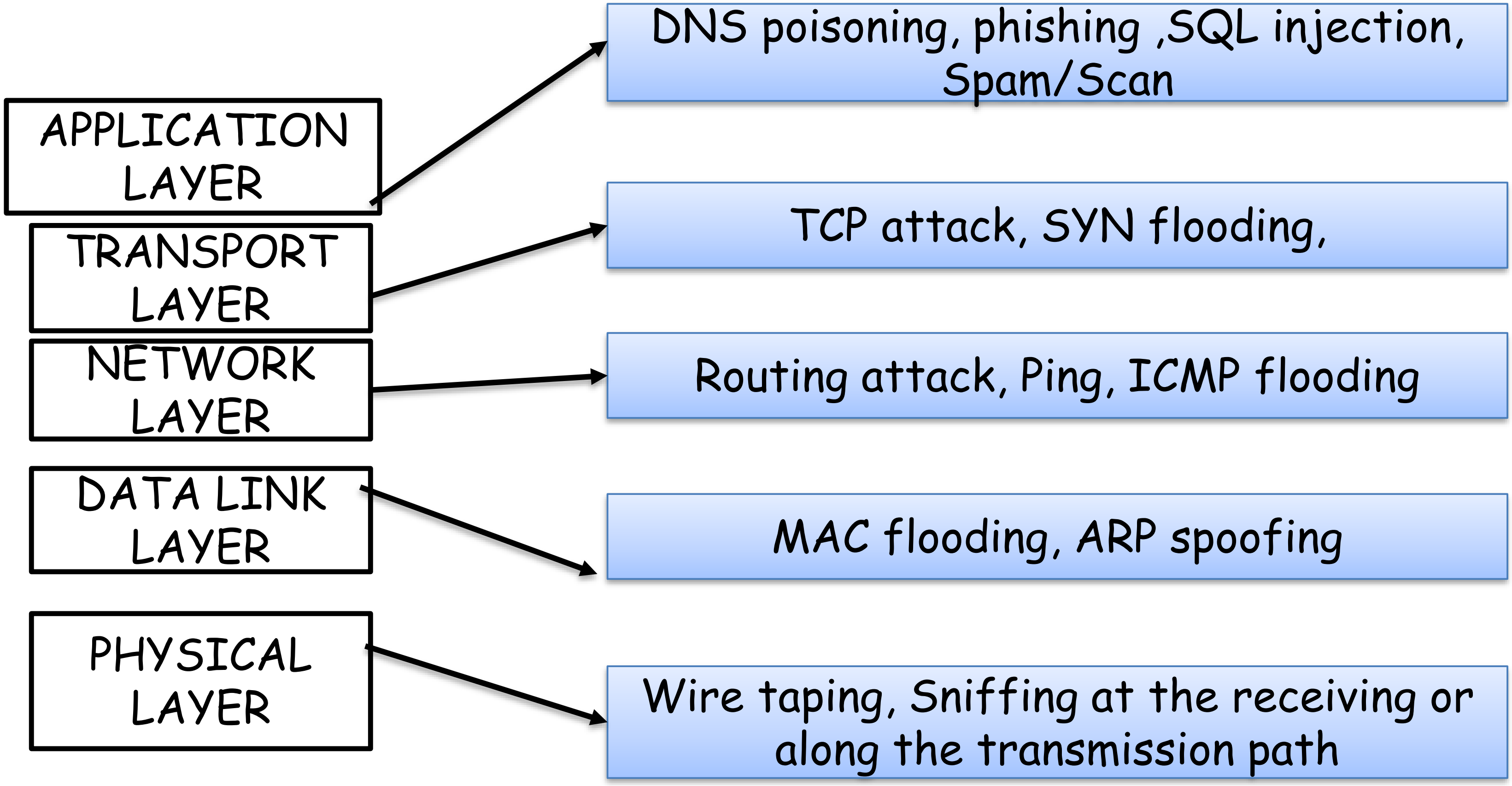


🟩 Message encrypted

□ Message in plaintext: Exposed

B	N	T	S	M

Attacks on different Network layers



APPLICATION LAYER

DNS poisoning, phishing ,SQL injection, Spam/Scan

TRANSPORT LAYER

TCP attack, SYN flooding,

NETWORK LAYER

Routing attack, Ping, ICMP flooding

DATA LINK LAYER

MAC flooding, ARP spoofing

PHYSICAL LAYER

Wire taping, Sniffing at the receiving or along the transmission path

Attacks on (Medium Access Control) Layer 2

- The data link layer (L2) is a weak link in terms of security.
- Switches are key components at L2 communications and they are also used for L3 communications.
- They are susceptible to many of the same L3 attacks as routers, and
- Many unique network attacks, which include
  - CAM table poisoning
  - CAM table overflow
  - VLAN hopping
  - ARP Spoofing (ARP Poisoning)
  - DHCP starvation

Attacks on MAC Layer

- MAC Layer:
  - Responsible for moving pkts from 1 NIC to another via a shared channel
- CAM Table
  - poisoning
  - **MAC Flooding:**

PORT	MAC
1	00:00:01:01:01:01
2	00:00:02:02:02:02
....	......
.....	....

  - overflows the switch MAC address table (CAM) forcing the switch to forward frames to all ports on a VLAN (much like a hub)
  - Catalyst CAM Table 16000 entries with 8 buckets (uses hash function)
  - MACOF tool generates random MAC/IP address combinations in order to overflow the CAM table
    - 155,000 MAC entries per minute

VLAN Hopping Attack

- VLAN Hopping Attack:
  - Attack used to gain unauthorized access to another Virtual LAN on a packet switched network
  - Attacker sends frames from one VLAN to another that would otherwise be inaccessible
  - Two methods:
    - Switch Spoofing
    - Double Tagging
      - send Dynamic Trunk protocol (DTP) packet