

First concepts

Terminology

What is Security?

- Definitions from the Amer. Herit. Dict. :
 - Freedom from risk or danger; safety. (NO!)
 - Measures adopted ... to prevent a crime such as burglary or assault. (ALMOST!)
- Network security measures:
 - Mechanisms to **prevent, detect, and recover** from network *attacks*, or for **auditing** purposes.

Terminology

- *Assets and liabilities*
- *Policies*
- *Security breeches*
- *Vulnerabilities*
- *Attacks*
- *Threats*
- *Threat Intensity*

A Secured Network

- A network is “secured” if it has deployed adequate measures for prevention of, detection of, and recovery from attacks.
 - Adequate = commensurate with the value of the network’s assets and liabilities, and the perceived threat intensity.
 - By Breno

Security Goals

- C onfidentiality
- I ntegrity
- A vailability

Confidentiality

- **Prevent** against:
 - adversarial capture (of information)
 - undue public disclosures
- **Audit** of data accesses
- **Detection** of unauthorized data access
- Retaliation (legal, PR, info. warfare)

Integrity: Data integrity + Authenticity

- **Prevent against** unauthorized data modification, and impersonation attacks
- **Detect** impersonation and/or undue data modification
- **Recover** from detected attacks
- **Audit** data modification, entity authentication

Availability

- Continuous service, quality of service, resource wastefulness reduction
 - Typical attack: DoS, DDoS
- Prevention by removal of bottlenecks
- **Detection** of attacks
- **Recovery** of service provision ability
- **Audit** of service requests.

Concrete Security Measures

- Securing an open network requires adoption of a myriad of measures:
 - Policies, audit and evaluation
 - Personnel training
 - Physical security/ EM emanation shielding
 - Authentication and access control
 - **Communication security:** Cryptography-based techniques.

Open Systems Interconnection

A standard-centric networking
model

Open Systems

- Open Systems:
 - general-purpose networks that support standardized communication protocols and may accommodate heterogeneous sub-networks transparently.
 - Corporate Intranets:
 - Ethernet, Token Ring and Wireless subnets.
 - Internet

Open Systems Interconnection Model

ISO's layered approach to standardization	
<i>7. Application layer</i>	<i>FTP, Telnet, SSH</i>
<i>6. Presentation layer</i>	<i>MIME, XDR, SSH</i>
<i>5. Session layer</i>	<i>NetBios, FTP, Telnet, SSH</i>
<i>4. Transport layer</i>	<i>TCP, UDP, SSL/TLS</i>
<i>3. Network layer</i>	<i>IP, ICMP, IPSEC</i>
<i>2. Data link layer</i>	<i>Ethernet, PPP, ISDN</i>
<i>1. Physical layer</i>	<i>pins, cabling, radio</i>

1-2. Physical/Data Link Layers

- Physical layer: Radio, fiber, cable, pins
- Data link layer orchestrates the signaling capabilities of the physical medium (unreliable, noisy channel) into reliable transmission of protocol data units (PDUs).
- PDUs contain control information, addressing data, and user data.
- Hardware-based encryption operates at 1+2.

3. Network Layer

- Exports a logical network interface, allowing for uniform addressing and routing over heterogeneous sub-networks.
 - E.g.: IP can route between Ethernet- and 802.11x - networks

4. Transport Layer

- Permits connection and connectionless associations. Connections enable reliable transmission of data streams.
- End-to-end security first becomes meaningful at this level.
 - Security associations: An *association* is either a connection or a connectionless transmission service at levels 4-7.

Levels 5 and Higher

- Application through session protocol layers.
 - Many network applications implement their own session management. Moreover, they typically depend on system libraries for presentation layer capabilities. Such applications, from a data-path viewpoint, may be considered a single layer: PDUs only typically appear at the session layer.

Example: SSH

- SSH provides provides services at all topmost three OSI layers.
 - Application: Terminal/file transfer
 - Presentation: Encryption
 - Session: Connection, synchronization
- Only at the session layer the data (encrypted buffers of user input) gets first packaged into a ***protocol data unit*** for transmission.

TCP/IP networking model

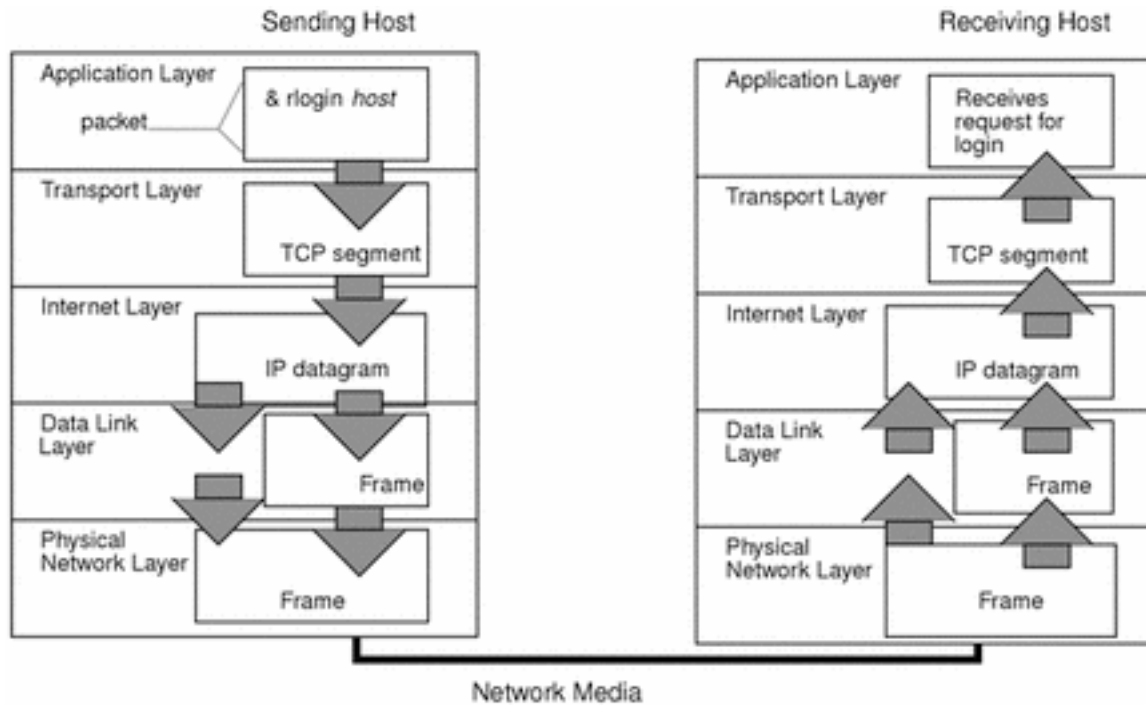
A data-path centric model

TCP/IP network model

(≠ TCP/IP Protocol)

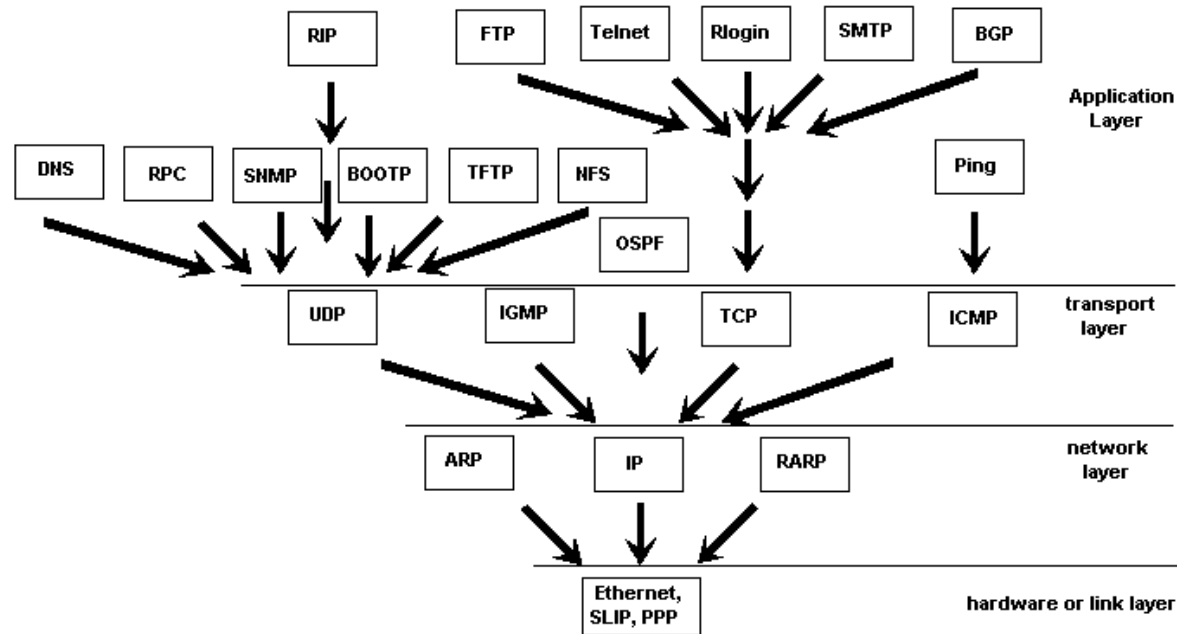
TCP/IP Application Layer	7. OSI Application
	6. OSI Presentation
	5. OSI Session
TCP/IP Transport Layer	4. OSI Transport
TCP/IP Network Layer	3. OSI Network
TCP/IP Data Link Layer	2. OSI Data Link Layer
TCP/IP Physical Layer	1. OSI Physical Layer

Protocol PDU Wrapping



Protocol Dependencies

Protocol Wrapper Dependencies and Network Layers



Fitting Security

How security measures fit into the
network models

Network Configuration

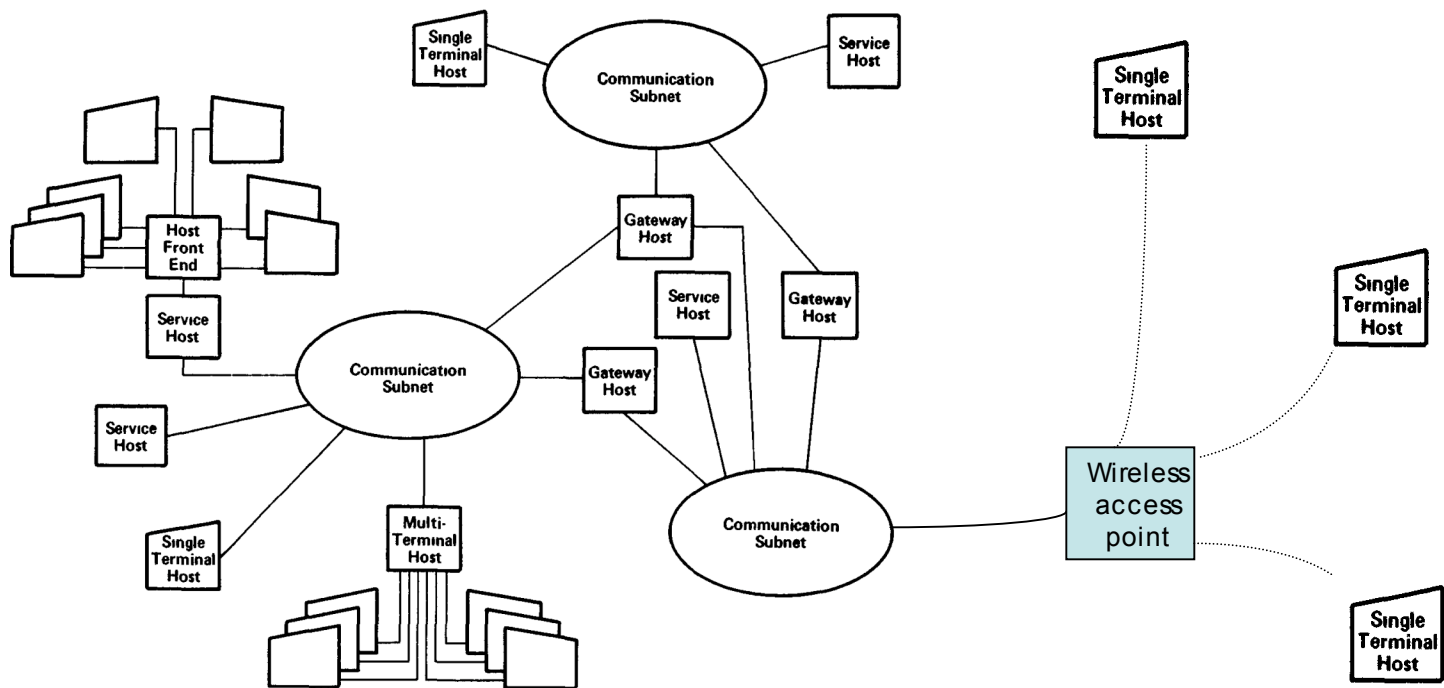
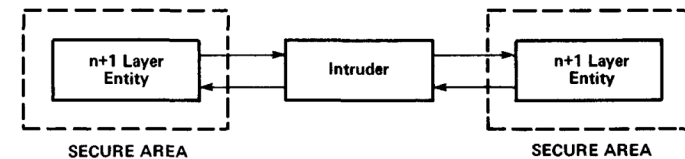
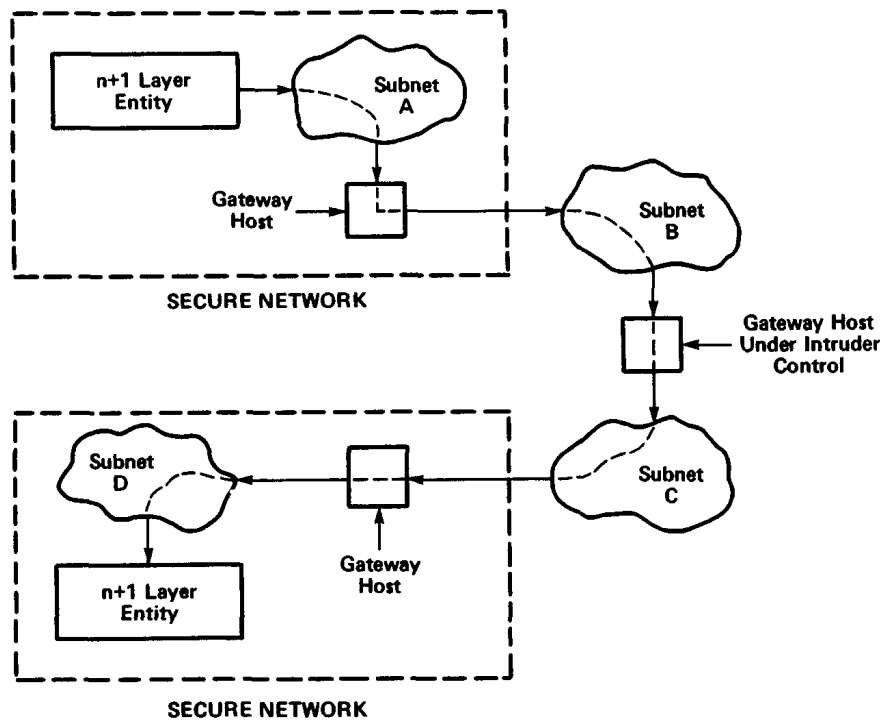


Figure 2. The network model.

Association Model

- An association is either a connectionless data transmission service or a connection at any of OSI layers 4-7, or TCP/IP application /transport layers
- An N-association is the data-path through which N+1 entities communicate:
 - Generally at session layer or below.
 - N+1-layer data packaged into N-PDUs

Association Model (2)



The association model simplifies the network environment, while still capturing the essential elements needed for security design.

Figure 5. Intruder in internetwork environment.

Security at levels 1 - 3

- Implemented at the host/network interface level (lack notion of association): Link-to-link security.
- Encryption/authentication requires operations at each network node.
- Each network node must be trusted.
 - Impractical for Open Systems?

Security protocols ≤ 3

- Many VPN technologies work at level 2
 - PPTP, L2F, L2TP
 - Rationale: Directed at dial-up VPN networks, (PPP is level-2). Provide service to a variety of network-level protocols, such as IP or IPX.
- IPSEC works at level 3, essentially extends IPv6/IPv4.

Security above level 3

- Most flexible security measures
- End-to-end security: The security policies and mechanisms can be based on associations between entities (applications, processes, connections), as opposed to host-based:
 - In multi-user environments, or when hosts are not physically secure, host-based policies are not sufficiently fine-grained.

Summary

- Security measures can take three main forms:
 1. End-to-end security at the TCP/IP application layer (5-7 OSI model layers)
 2. End-to-end security at the (TCP/IP,OSI) transport layer
 3. Link-to-link security at the network, data-link and physical layers.

Attacks

A taxonomy

Attack Types

And their impact on end-to-end
communication security
mechanisms

Passive Attacks

- Observation of N+1-layer data in an N-layer PDU: *release of data contents*, or *eavesdropping*
- Observation of control/ address information on the N-PDU itself: *traffic analysis*.
- Transport/network boundary = End-to-end/ link-to-link boundary.
 - Traffic analysis is least effective if $N+1 = 4$.

Active Attacks

- Impersonation
- Packet injection (attacker-generated PDU)
- Packet deletion/delay
- Packet modification/re-ordering
- Replay attacks
- If a breach can be achieved by both active and passive attacks, which is more powerful? (problematic)