



---

# Chapter 8

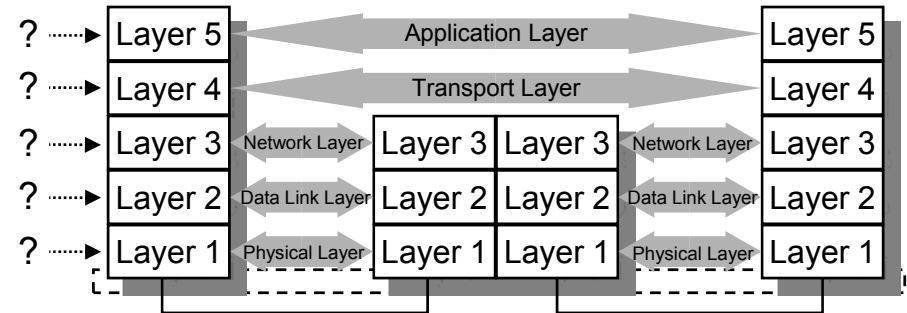
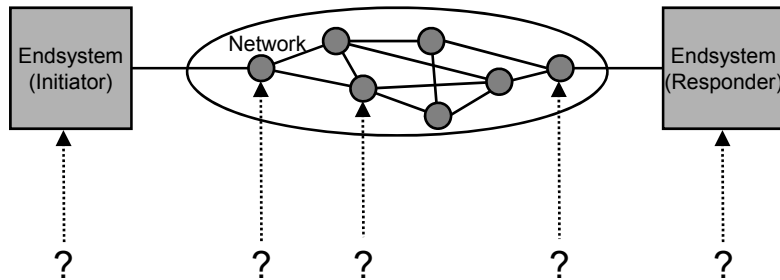
## Integrating Security Services into Communication Architectures

- ❑ Models
- ❑ VPN

# Motivation: What to do where?



- Analogous to the methodology of security analysis, there are *two dimensions* guiding the integration of security services into communications architectures:



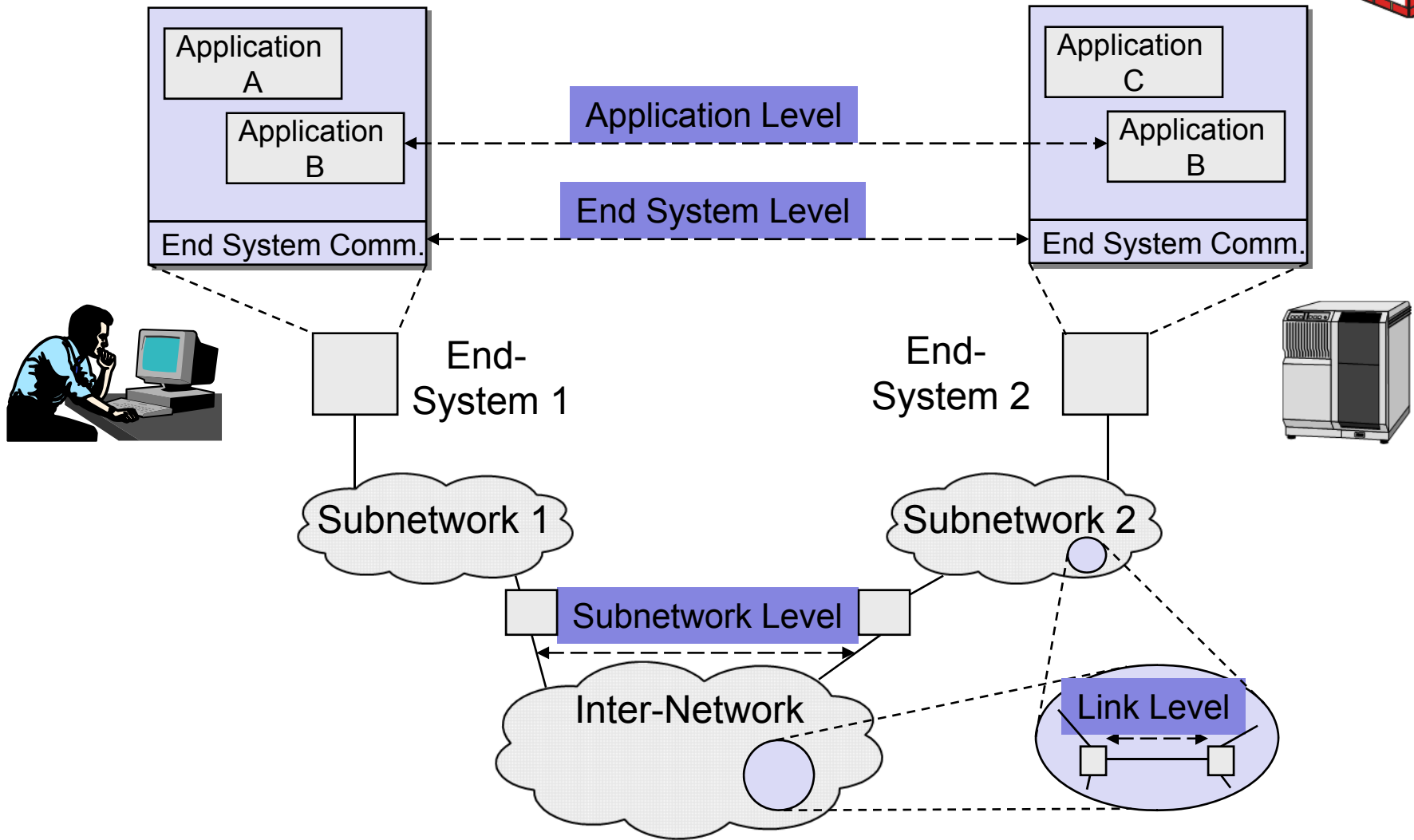
## Dimension 1:

Which security service should be realized in which node?

## Dimension 2:

Which security service should be realized in which layer?

# A Pragmatic Model for Secured & Networked Computing



# Considerations Regarding Specific Levels

---



- ❑ **Application** – *A piece of software that accomplishes some specific task, e.g. electronic mail, web service, word processing, data storage, etc*
  - ❑ A security service is application specific, e.g. access control for a networked file store
  - ❑ A security service needs to traverse application gateways, e.g. integrity and / or confidentiality of electronic mail
  - ❑ Semantics of data is important, e.g. for non-repudiation services
  - ❑ It is beyond the reach of a user / application programmer to integrate security at a lower level
  
- ❑ **End system** – *One piece of equipment, anywhere in the range from personal computer to server to mainframe computer*
  - ❑ This level is appropriate when end systems are assumed to be trusted and the communication network is assumed to be untrusted
  - ❑ Security services are transparent to applications
  - ❑ The management of security services can be more easily given in the hands of one system administrator

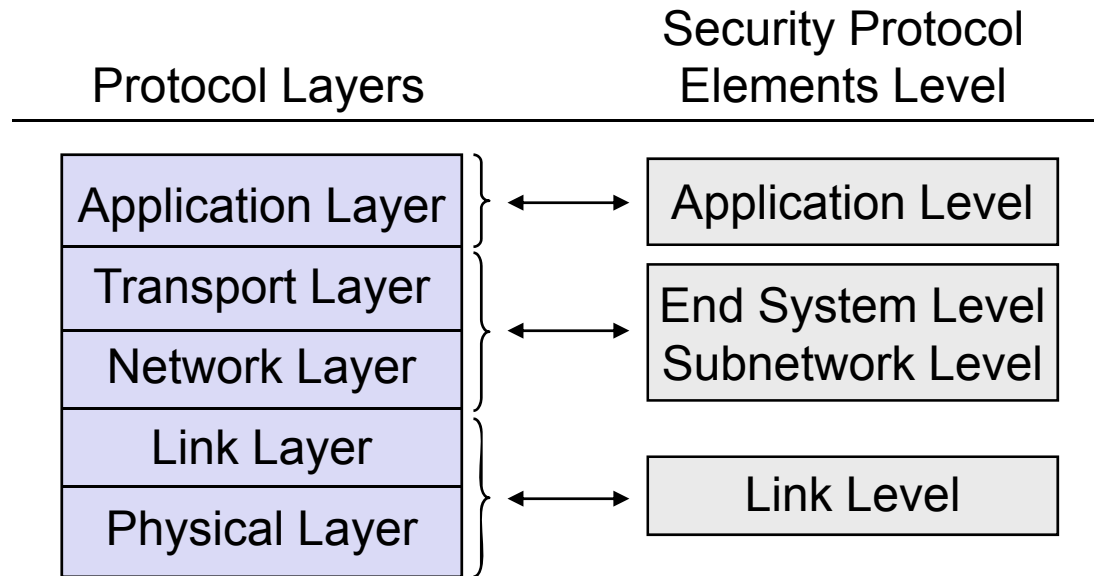
# Considerations Regarding Specific Levels

---



- ❑ **Subnetwork** – *A collection of communication facilities being under the control of one administrative organization, e.g. a LAN, campus network, etc*
  - ❑ Even if security implemented on this level might be implemented in the same protocol layer like for the end system level, these should not be mixed up:
    - With security implemented on the subnetwork level, usually the same protection is realized for **all end systems** of that subnetwork
  - ❑ It is very common, that a subnetwork close to an end system is considered equally trusted, as there are on the same premises and administered by the same authorities
  - ❑ In most situations there are far less subnetwork gateways to be secured than there are end systems
  
- ❑ **Link** – *A local network such as an Ethernet or a WLAN*
  - ❑ If there are relatively few untrusted links, it might be sufficient and as well easier and cheaper to protect the network on the link level
  - ❑ Furthermore the link level allows to make use of specific protection techniques, like spread spectrum or frequency hopping techniques
  - ❑ Traffic flow confidentially usually demands for link level protection

# Relationships Between Layers & Requirements Levels



- ❑ The relations between protocol layers and the protocol element security requirements levels are not one-to-one:
  - ❑ Security mechanisms for fulfilling both the end system and the subnetwork level requirements can be either realized in the transport and / or the network layer
  - ❑ Link level requirements can be met by integrating security mechanisms or using “special functions” of the either the link layer and / or the physical layer

# General Considerations for Architectural Placement

---



- ❑ *Number of protection points:*
  - ❑ Placing security at the application level requires security to be implemented in every sensitive application and every end system
  - ❑ Placing security at the link level requires security to be implemented at the end of every network link which is considered to be less trusted
  - ❑ Placing security in the middle of the architecture will tend to require security features to be installed at fewer points
- ❑ *Protocol header protection:*
  - ❑ Security protection at higher levels can not protect protocol headers of lower protocol layers
  - ❑ The networking infrastructure might need to be protected as well
- ❑ *Source / sink binding:*
  - ❑ Security services like data origin authentication and non-repudiation depend upon association of data with its source or sink
  - ❑ This is most efficiently achieved at higher levels, especially the application level

# Integration into Lower Protocol Layers vs. Applications

---



- ❑ Benefits of integrating security services into lower network layers:
  - ❑ *Security:*
    - The network itself also needs to be protected
    - Security mechanisms realised in the network elements (esp. in hardware) are often harder to attack for network users
  - ❑ *Application Independence:*
    - Basic network security services need not be integrated into every single application
  - ❑ *Quality of Service (QoS):*
    - QoS preserving scheduling of the communication subsystem can also schedule encryption of co-existing data streams
    - Example: simultaneous voice call and FTP transfer
  - ❑ *Efficiency:*
    - Hardware support for computationally intensive encryption / decryption can be easier integrated into protocol processing

# Integration into End Systems vs. Intermediate Systems

---



- ❑ Integration into end systems:
  - ❑ Can be done generally either on the application or end system level
  - ❑ In some special cases also a link level protection might be appropriate, e.g. when using a modem to connect to a dedicated device
- ❑ Integration into intermediate systems
  - ❑ Can be done on all four levels:
    - Application / “end system” level: for securing management interfaces of intermediate nodes, not for securing user data traffic
    - Subnetwork / link level: for securing user data traffic
- ❑ Depending on the security objectives an integration in both end systems and intermediate systems might be appropriate

# Virtual Private Networks

---



- ❑ Various definitions of the term *virtual private network (VPN)*:
  - ❑ A private network constructed within a public network infrastructure, such as the global Internet
  - ❑ A communications environment in which access is controlled to permit peer connections only within a defined community of interest, and is constructed through some form of partitioning of a common underlying communications medium, where this underlying communications medium provides services to the network on a non-exclusive basis
  - ❑ A restricted-use, logical computer network that is constructed from the system resources of a relatively public, physical network (such as the Internet), often by using encryption, and often by tunneling links of the virtual network across the real network [RFC2828]
  - ❑ Remark: the later two definitions explicitly incorporate security properties (controlled access, encryption) while the first one does not

*“Sure, it’s a lot cheaper than using your own frame relay connections, but it works about as well as sticking cotton in your ears in Times Square and pretending nobody else is around.” (Wired Magazine Feb. 1998)*

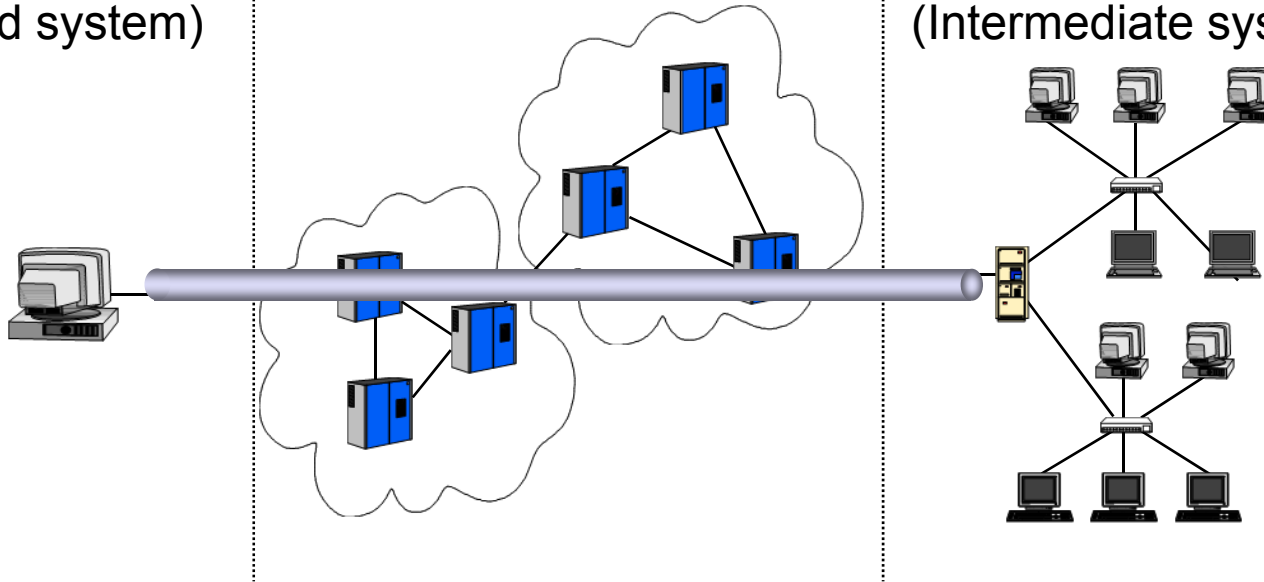
# Virtual Private Networks



Private Network  
(End system)

Public Network

Private Network  
(Intermediate system)



---

Authentication Relation

---

End system ↔ End system

End system ↔ Intermediate system

Intermediate ↔ Intermediate system

---

Application for securing

---

User Channels

Management Interfaces,  
Accounting

Network Operation: Signaling  
Routing, Accounting, ...

# Summary (what do I need to know)

---



- ❑ Horizontal vs. vertical mapping of security services
  - ❑ Technical requirements
  - ❑ Social and administrative constraints
  
- ❑ Virtual private networks
  - ❑ Dedicated lines vs. tunneling
  - ❑ Intermediate systems (supporting entire private networks) or end systems

# Additional References

---



- [RFC2828] R. Shirey. *Internet Security Glossary*. RFC 2828, 2000.
- [FH98a] P. Ferguson, G. Huston. *What is a VPN?* The Internet Protocol Journal, volume 1, no. 1&2, Cisco Systems. 1998.
- [ATM99a] ATM Forum. *ATM Security Specification Version 1.0*. AF-SEC- 0100.000, February, 1999.