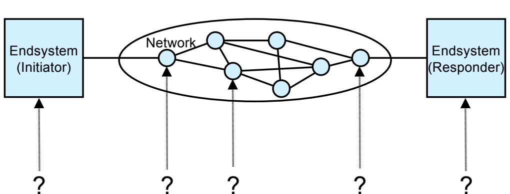
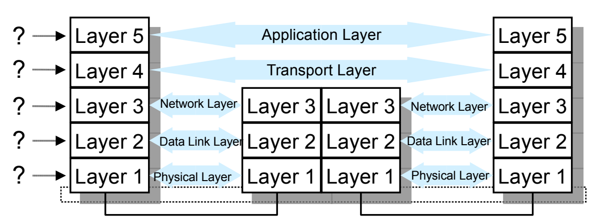
Network Security

Chapter 10
Integrating Security Services into Communication Architectures

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:

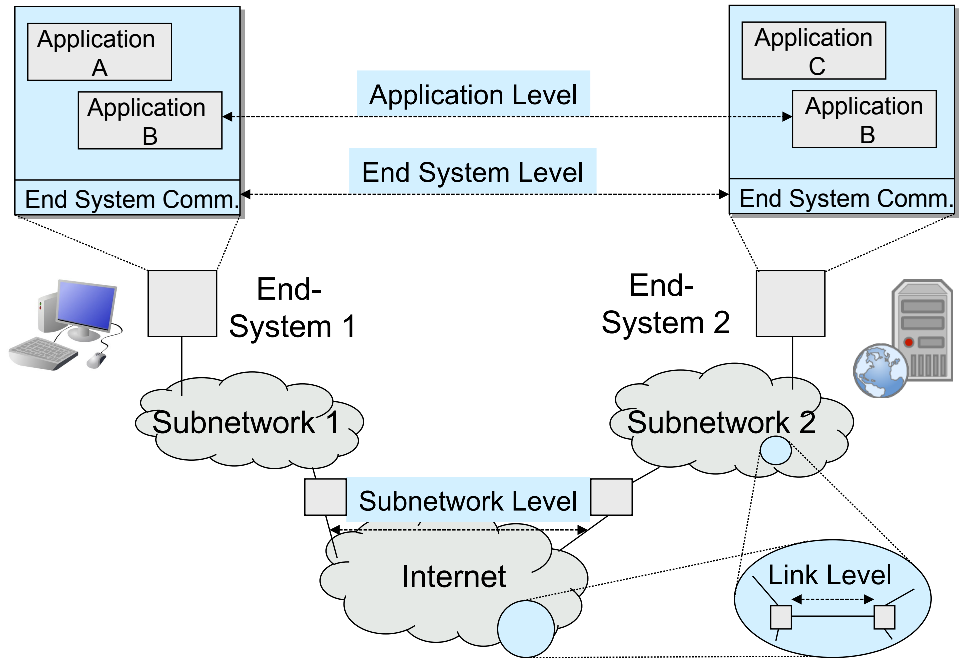




<u>Dimension 1:</u>
Which security service should be realized in which node?

<u>Dimension 2:</u>
Which security service should be realized in which layer?

A Pragmatic Model for Secured & Networked Computing (1)



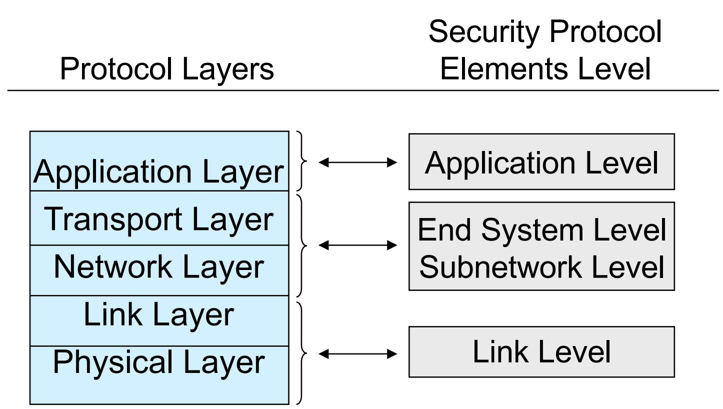
A Pragmatic Model for Secured & Networked Computing (2)

- *Application:*
  - A piece of software that accomplishes some specific task, e.g. electronic email, web service, word processing, data storage, etc.
- *End System:*
  - One piece of equipment, anywhere in the range from personal computer to server to mainframe computer
  - For security purposes one end system usually has one policy authority
- *Subnetwork:*
  - A collection of communication facilities being under the control of one administrative organization, e.g. a LAN, campus network, WAN, etc.
  - For security purposes one subnetwork usually has one policy authority
- *Internet:*
  - A collection of inter-connected subnetworks
  - In general, the subnets connected in an inter-network have different policy authorities

A Pragmatic Model for Secured & Networked Computing (3)

- There are four levels at which distinct requirements for security protocol elements arise:
  - *Application level:*
    - Security protocol elements that are application dependent
  - *End system level:*
    - Provision of protection on an end system to end system basis
  - *Subnetwork level:*
    - Provision of protection over a subnetwork or an inter-network which is considered less secure than other parts of the network environment
  - *Link level:*
    - Provision of protection internal to a subnetwork, e.g. over a link which is considered less trusted than other parts of the subnetwork environment

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 (1)

- *Traffic mixing:*
  - As a result of multiplexing, there is greater tendencies at lower levels to have data items from different source/destination-users and / or applications mixed in one data stream
  - A security service realized at one layer / level will treat the traffic of that layer / level in an equal manner, resulting in inadequate control over security mechanisms for users and applications
  - If a security policy demands for a more differentiated treatment, it should be better realized at a higher level
- *Route knowledge:*
  - At lower levels, there tends to be more knowledge about the security characteristics of different routes and links
  - In environments, where such characteristics vary significantly, placing security at lower levels can have effectiveness and efficiency benefits
  - Appropriate security services can be selected on a subnetwork or link basis eliminating cost for security, where protection is unnecessary

General Considerations for Architectural Placement (2)

- *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

Considerations Regarding Specific Levels (1)

- *Application level:*
  - This level might be the only appropriate level, for example because:
    - 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 level:*
  - This level is appropriate when end systems are assumed to be trusted and the communication network is assumed to be untrusted
  - Further advantages of end system level security:
    - 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 (2)

- *Subnetwork level:*
  - 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 level:*
  - 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

Human User Interactions

- Some network security services involve direct interaction with a human user, the most important one being authentication
- Such interactions do not cleanly fit into any of the architectural options presented so far, as the user is external to the communication facilities
- Communications supporting authentication can be realized in one of the following manners:
  - *Locally:*
    - The human user authenticates to the local end system
    - The end system authenticates itself to the remote end system and advises the user identity
    - The remote system has to trust the local end system
  - *Involving protocol elements at the application layer:*
    - The user passes some authentication information to the local system which is securely relayed to the remote system
  - *Combining the above means:*
    - Example: Kerberos

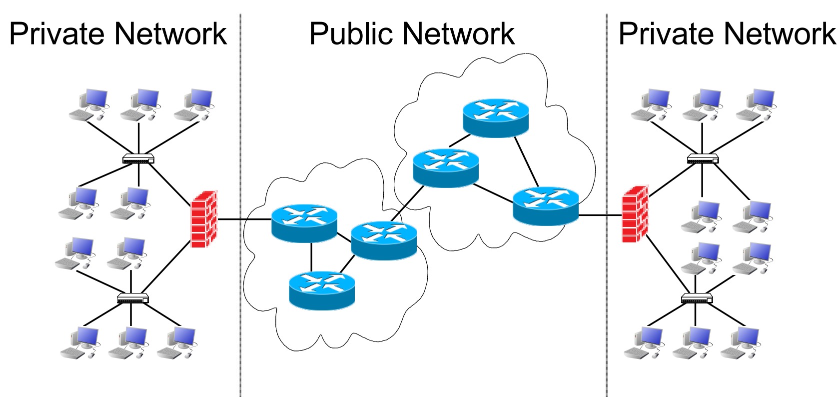
Integration into Lower Protocol Layers vs. Applications

- 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

Example: Authentication Relations in Inter-Networks



Authentication Relation	Application for securing
Endsystem ↔ Endsystem	User Channels
Endsystem ↔ Intermediate System	Management Interfaces, Accounting
Intermediate ↔ Intermediate System	Network Operation: Signaling Routing, Accounting, ...

Conclusion

- Integration of security services into communications architectures is guided by two main questions:
  - Which security service into which node?
  - Which security service into which layer?
- These design choices can also be guided by looking at a pragmatic model of networked computing which distinguishes four different levels on which security services may be realized:
  - Application / end system / subnetwork / link level
- As there are various reasons for and against each option, there is no single solution to this design problem
- In this course we will, therefore, study some examples of security services integration into network architectures in order to better understand the implications of the design choices made