
ESTD1845
QUEEN'S
UNIVERSITY
BELFAST

Network Security Architecture – Part 1

Dr. Sandra Scott-Hayward

CSC3064 Lecture 04

School of Electronics, Electrical Engineering and Computer Science

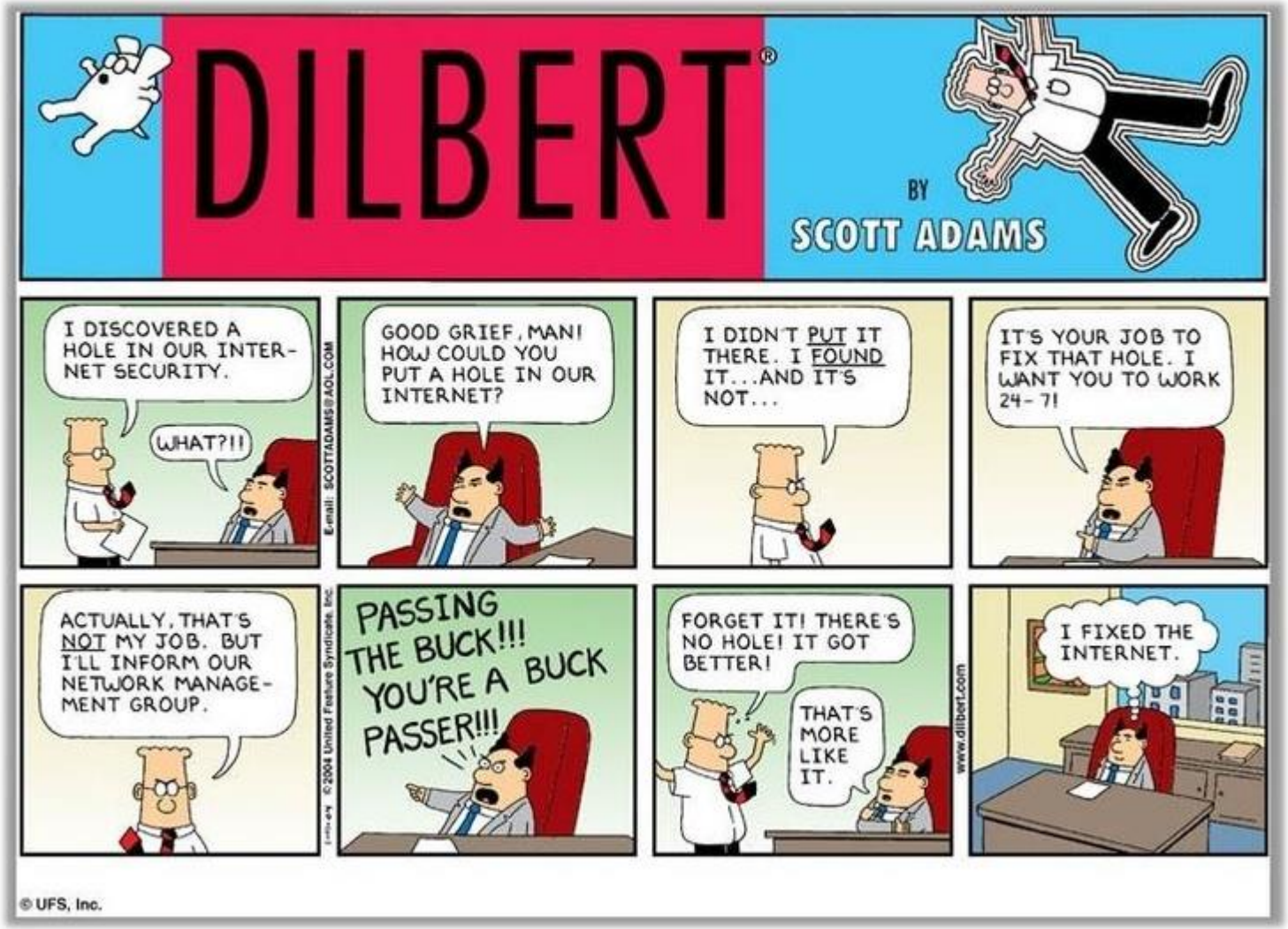
Session Overview

- Integrating security services into network architectures
  - Considerations for architectural placement
  - Considerations with respect to specific levels
  - Example network models

References:
Harris, Shon. *CISSP all-in-one exam guide*. McGraw-Hill, Inc., 2010.
Schäfer, Günter, and Michael Rossberg. *Security in Fixed and Wireless Networks*. John Wiley & Sons, 2016.

QUEEN'S UNIVERSITY BELFAST

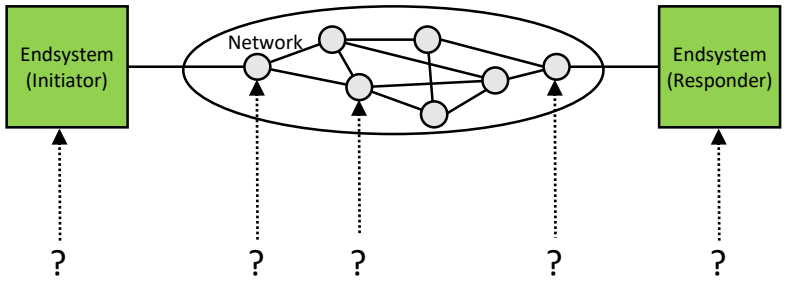
Securing the Network …

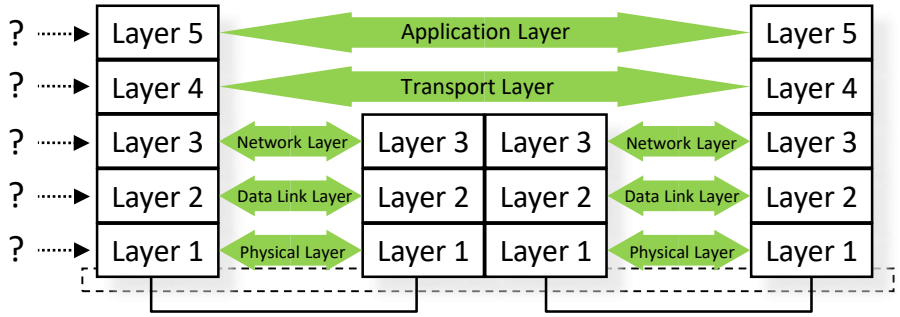


QUEEN'S UNIVERSITY BELFAST

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:

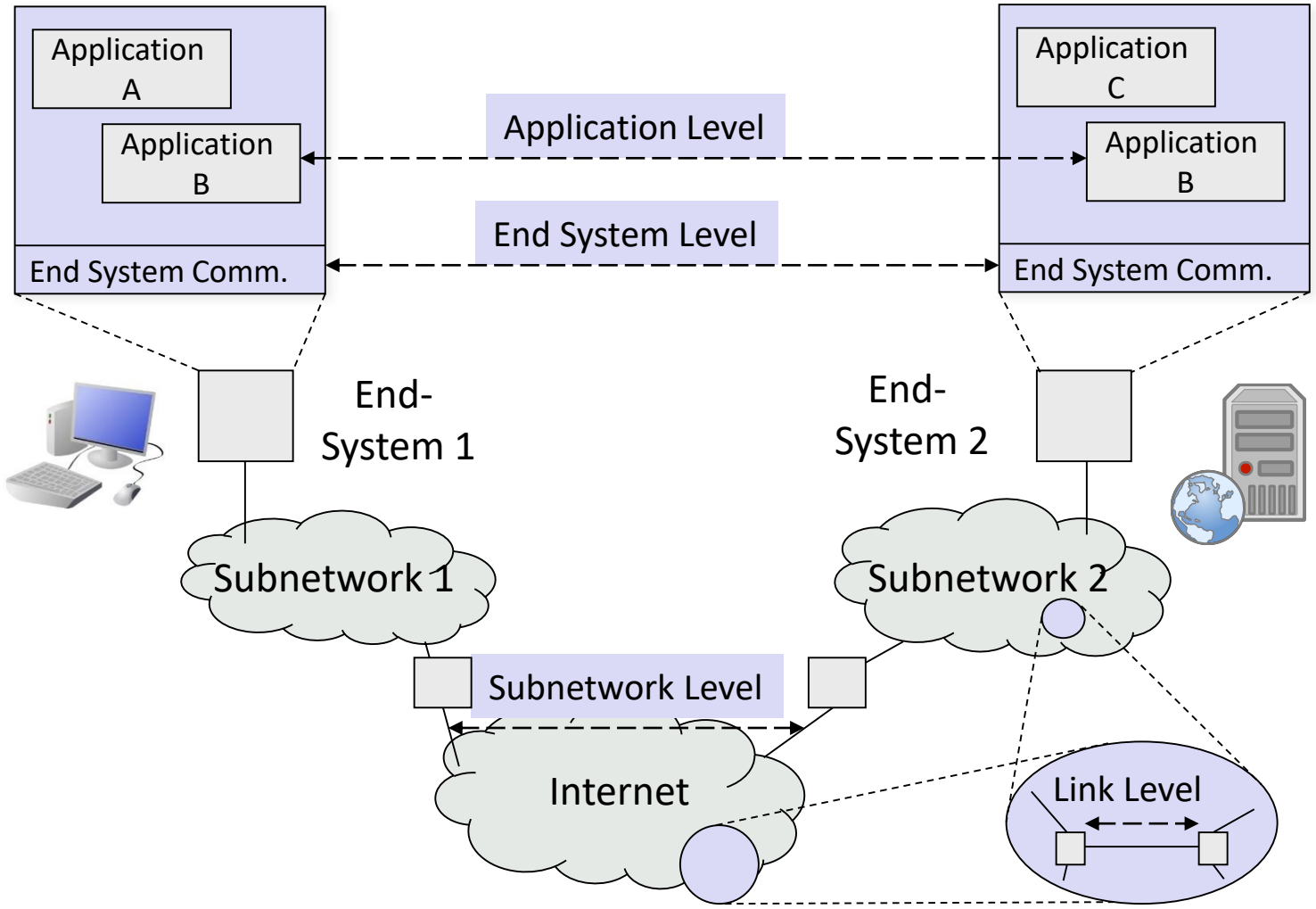
Which security service should be realized in which node?

Dimension 2:

Which security service should be realized in which layer?

QUEEN'S UNIVERSITY BELFAST

A practical model for secured & networked computing (1)



QUEEN'S UNIVERSITY BELFAST

A practical model for secured & networked computing (2)

Application:

- A piece of software that accomplishes some specific task, e.g. email, web service, file transfer, 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 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 practical 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:

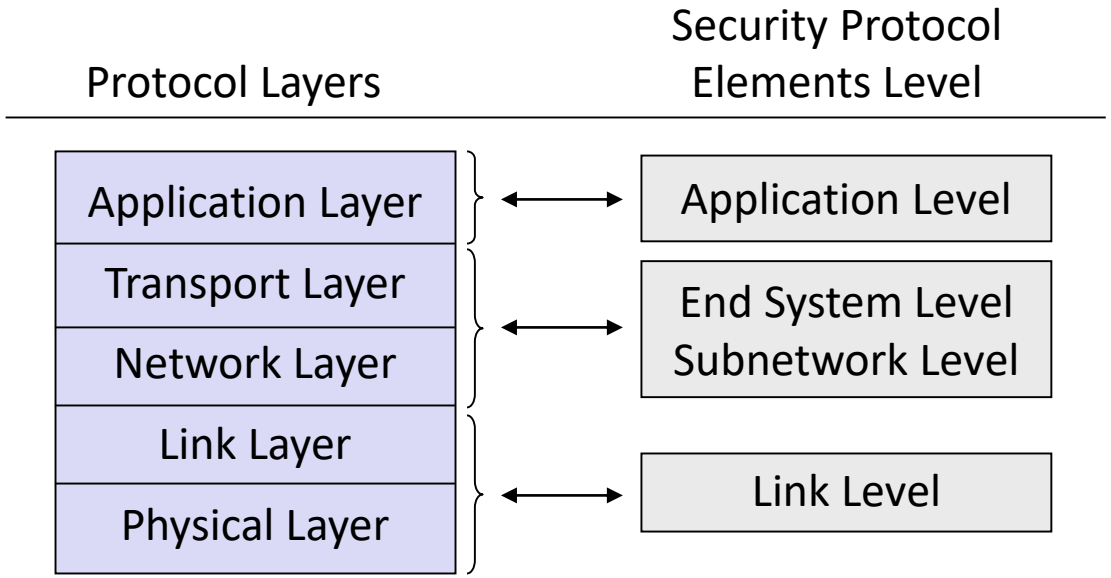
Provision of protection over a subnetwork or an inter-network, which is considered to be less secure than other parts of the network environment

Link level:

Provision of protection internal to a subnetwork, e.g. over a link, which is considered to be less trusted than other parts of the subnetwork environment

QUEEN'S UNIVERSITY BELFAST

Relationships between layers and requirement levels

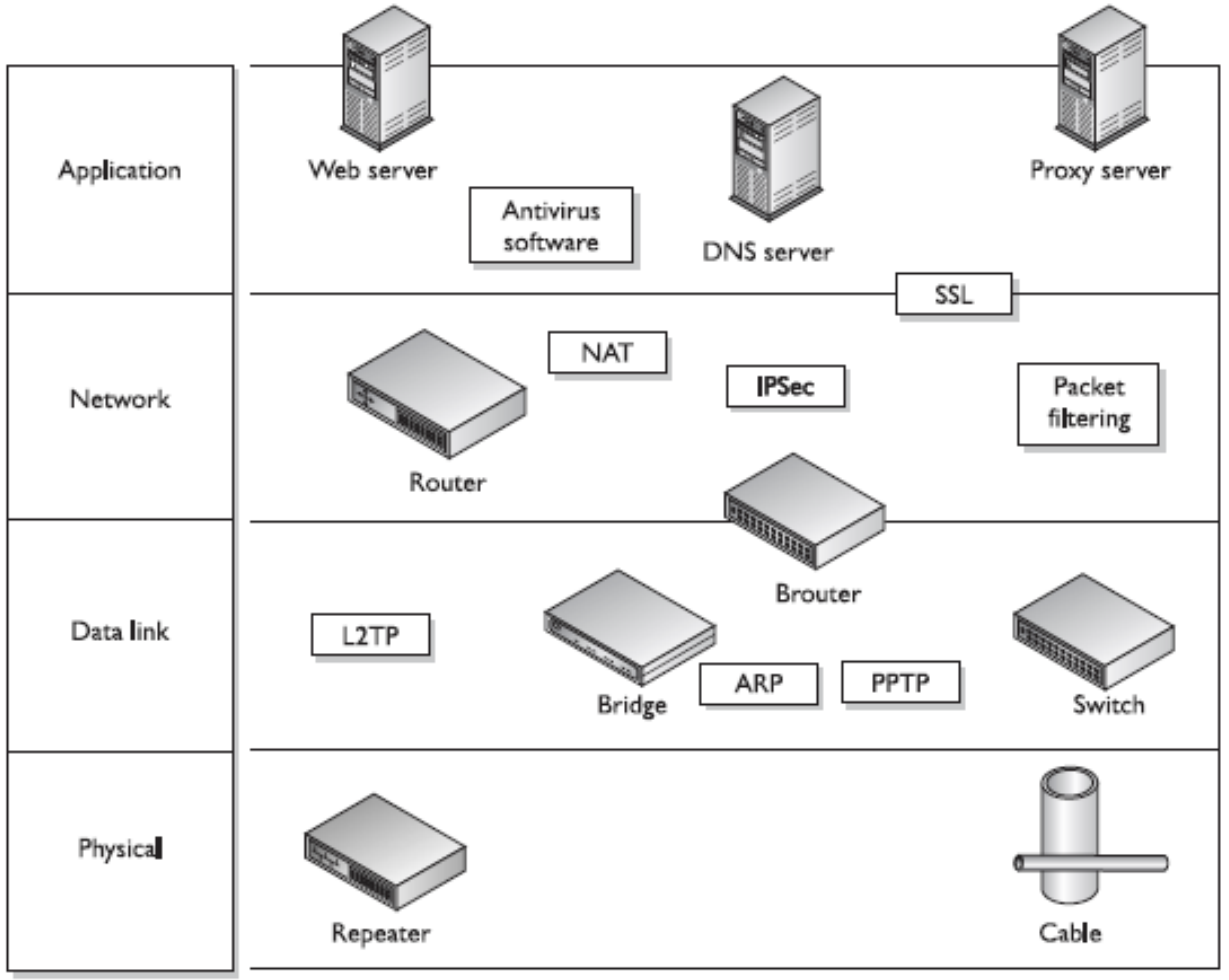


The relationship between protocol layers and the protocol element security requirement levels are not one-to-one:

- Security mechanisms for fulfilling both the end system and the subnetwork level requirements can either be realized in the transport and / or the network layer
- Link level requirements can be met by integrating security mechanisms or using “special functions” of either the link layer and / or the physical layer

QUEEN'S UNIVERSITY BELFAST

Devices and protocols and where they appear in the OSI model

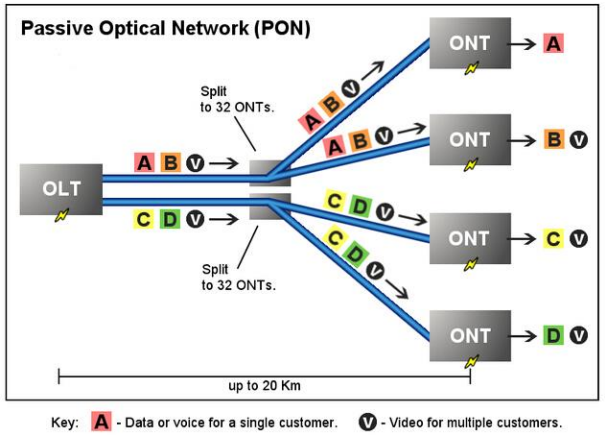


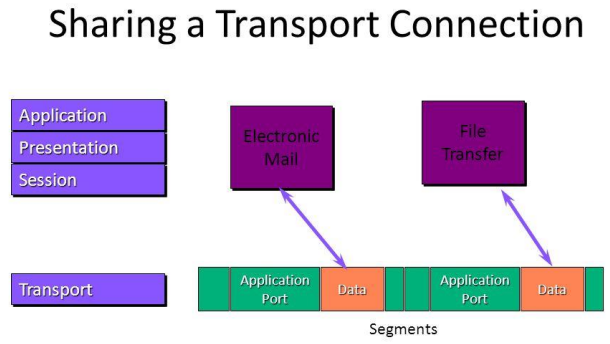
QUEEN'S UNIVERSITY BELFAST

General considerations for architectural placement (1)

Traffic mixing:

- As a result of multiplexing, there is a greater tendency 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 a more differentiated treatment, it is better to implement it at a higher level





QUEEN'S UNIVERSITY BELFAST

General considerations for architectural placement (2)

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 be more effective and efficient
- Appropriate security services can be selected on a subnetwork or link basis reducing the cost for security where protection is not required

Number of protection points:

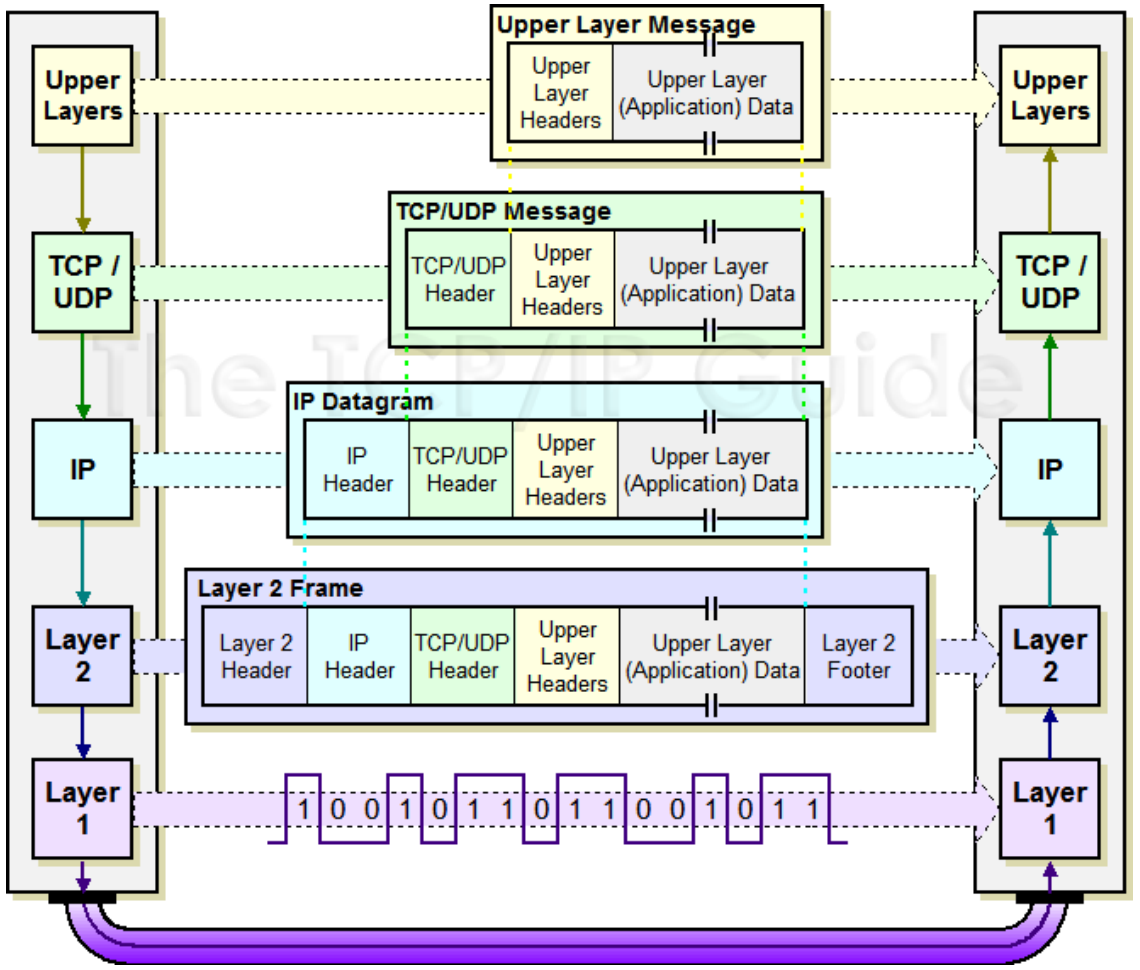
- Placing security at the application level requires security to be implemented in every sensitive application and every end system
- Placing security at the link level requires security to be implemented at the end of every network link which is considered to be less trusted
- Placing security in the middle of the architecture will tend to require security features to be installed at fewer points

QUEEN'S UNIVERSITY BELFAST

General considerations for architectural placement (3)

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



QUEEN'S UNIVERSITY BELFAST

General considerations for architectural placement (4)

Source / sink binding:

- Security services such as data origin authentication and non-repudiation depend upon association of data with its source or sink
- This is most efficiently achieved at higher levels, in particular the application level

QUEEN'S UNIVERSITY BELFAST

Considerations with respect to 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
- It is outside the control of a user / application programmer to integrate security at a lower level

QUEEN'S UNIVERSITY BELFAST

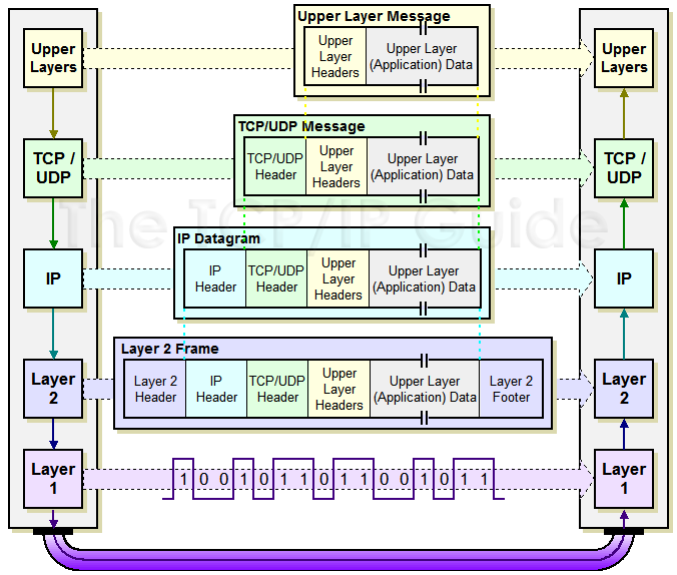
Considerations regarding specific levels (2)

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 handled by one system administrator

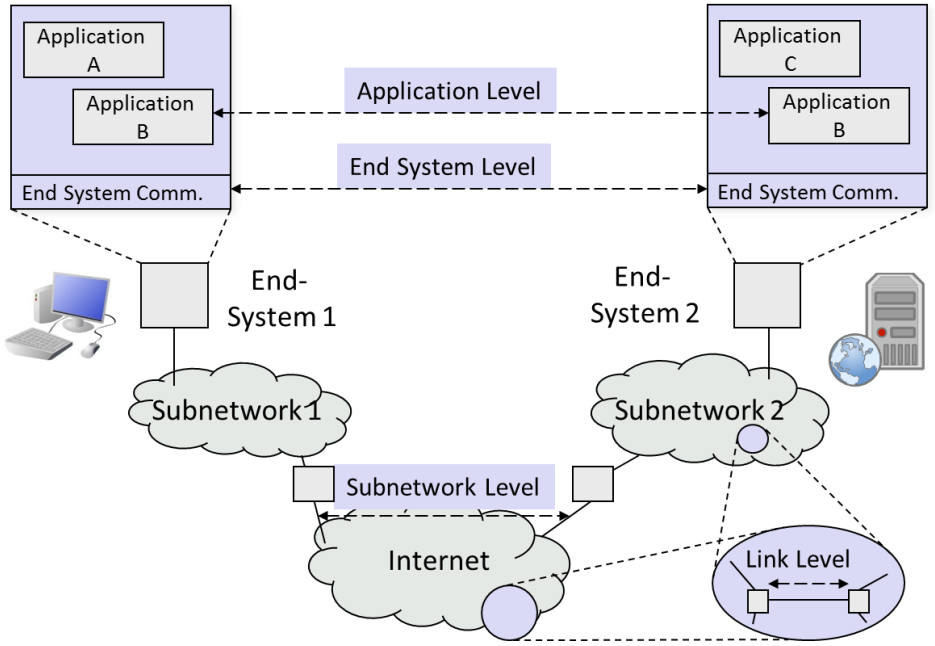


QUEEN'S UNIVERSITY BELFAST

Considerations regarding specific levels (3)

Subnetwork level:

- Even if security implemented at this level might be implemented in the same protocol layer as for the end system level, these should not be mixed up:
  - With security implemented at 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 they are on the same premises and administered by the same authorities
- In most situations, there are far fewer subnetwork gateways to be secured than there are end systems

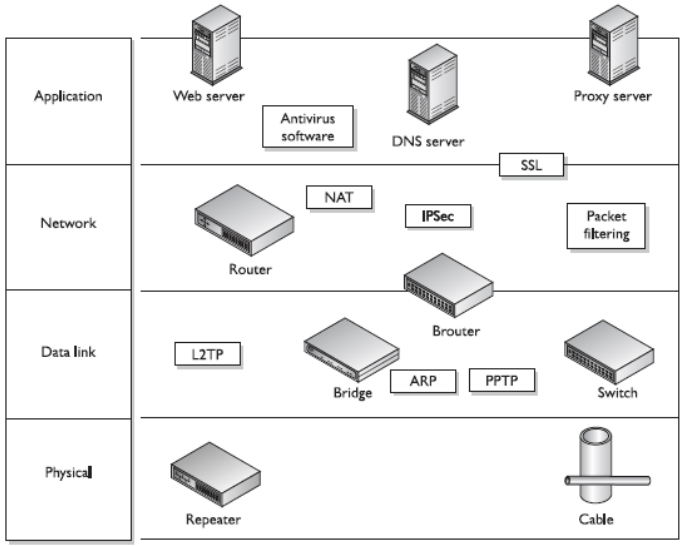


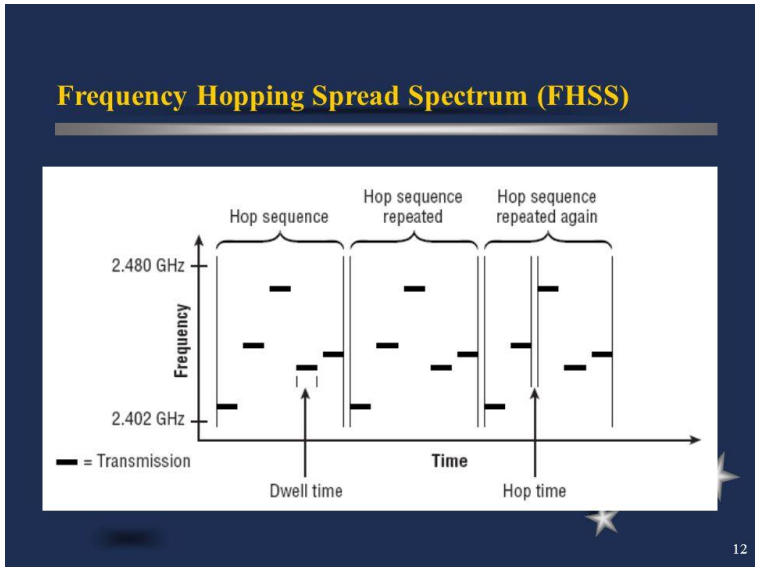
QUEEN'S UNIVERSITY BELFAST

Considerations regarding specific levels (4)

Link level:

- If there are relatively few untrusted links, it might be sufficient, easier and cheaper to protect the network at the link level
- Furthermore, the link level allows to make use of specific protection techniques, such as spread spectrum or frequency hopping techniques
- Traffic flow confidentially usually demands link level protection





QUEEN'S UNIVERSITY BELFAST

Human user interactions (1)

- 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

QUEEN'S UNIVERSITY BELFAST

Human user interactions (2)

- Communications supporting authentication can be realized in one of the following ways:

  Locally:

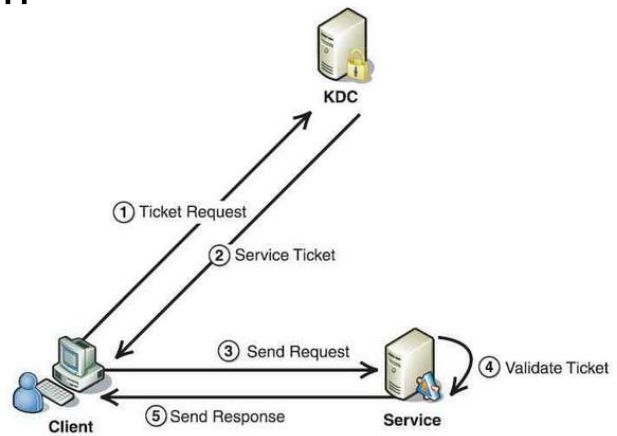
  - The human user authenticates to the local end system
  - The end system authenticates itself to the remote end system and advises the user identity
  - The remote system has to trust the local end system

  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

  The combination of these is, for example:

  - Kerberos



QUEEN'S UNIVERSITY BELFAST

Integration into lower protocol layers vs. applications

Benefits of integrating security services into lower network layers:

Stronger Security:

- The network itself also needs to be protected
- Security mechanisms realised in the network elements (esp. in hardware) are often harder for network users to attack

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

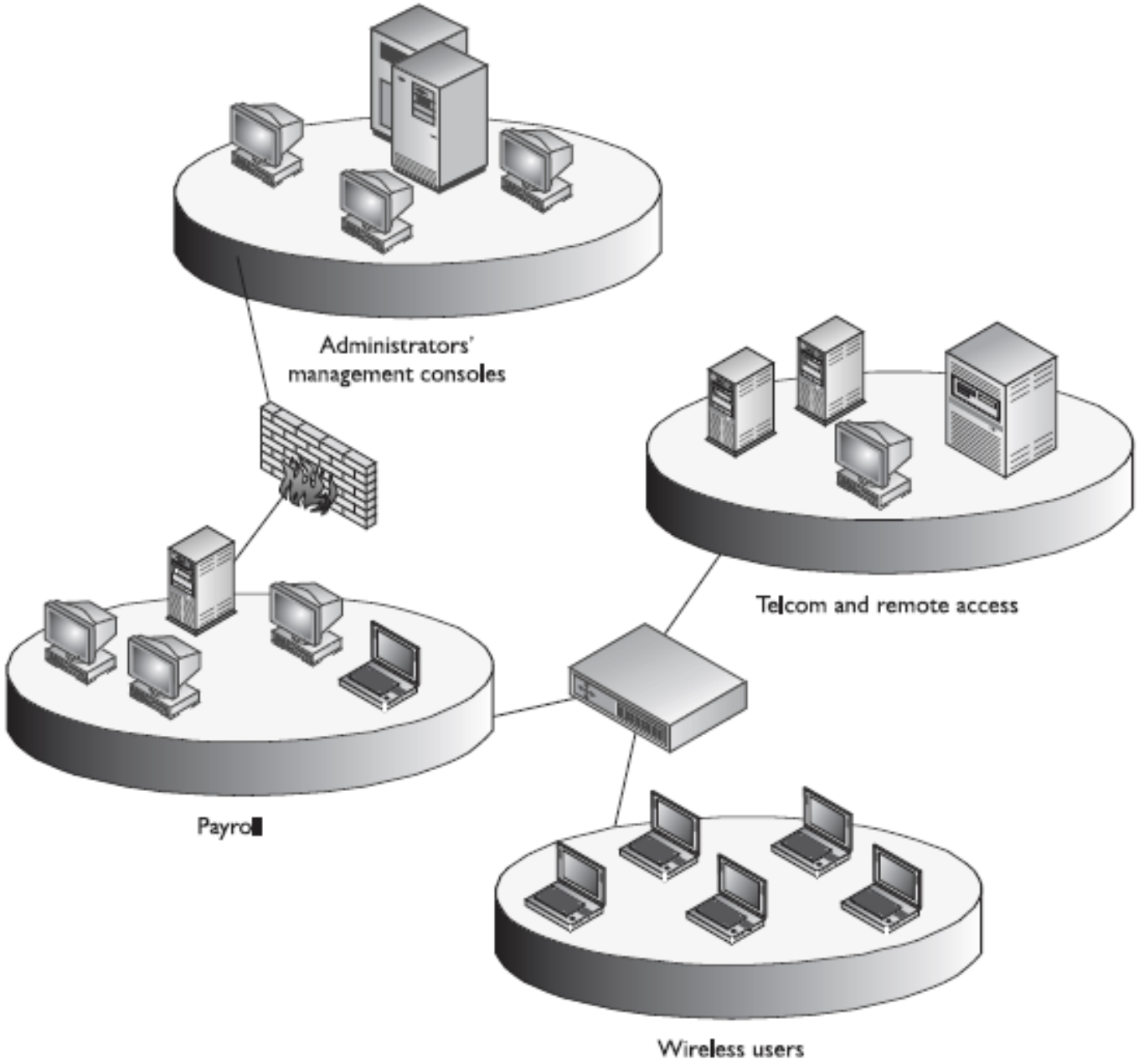
Efficiency:

- Hardware support for computationally intensive encryption / decryption can be more easily integrated into protocol processing

QUEEN'S UNIVERSITY BELFAST

Example Network Models (1)

Illustrating separate sub-networks for different functions of an organisation requiring different security policies.

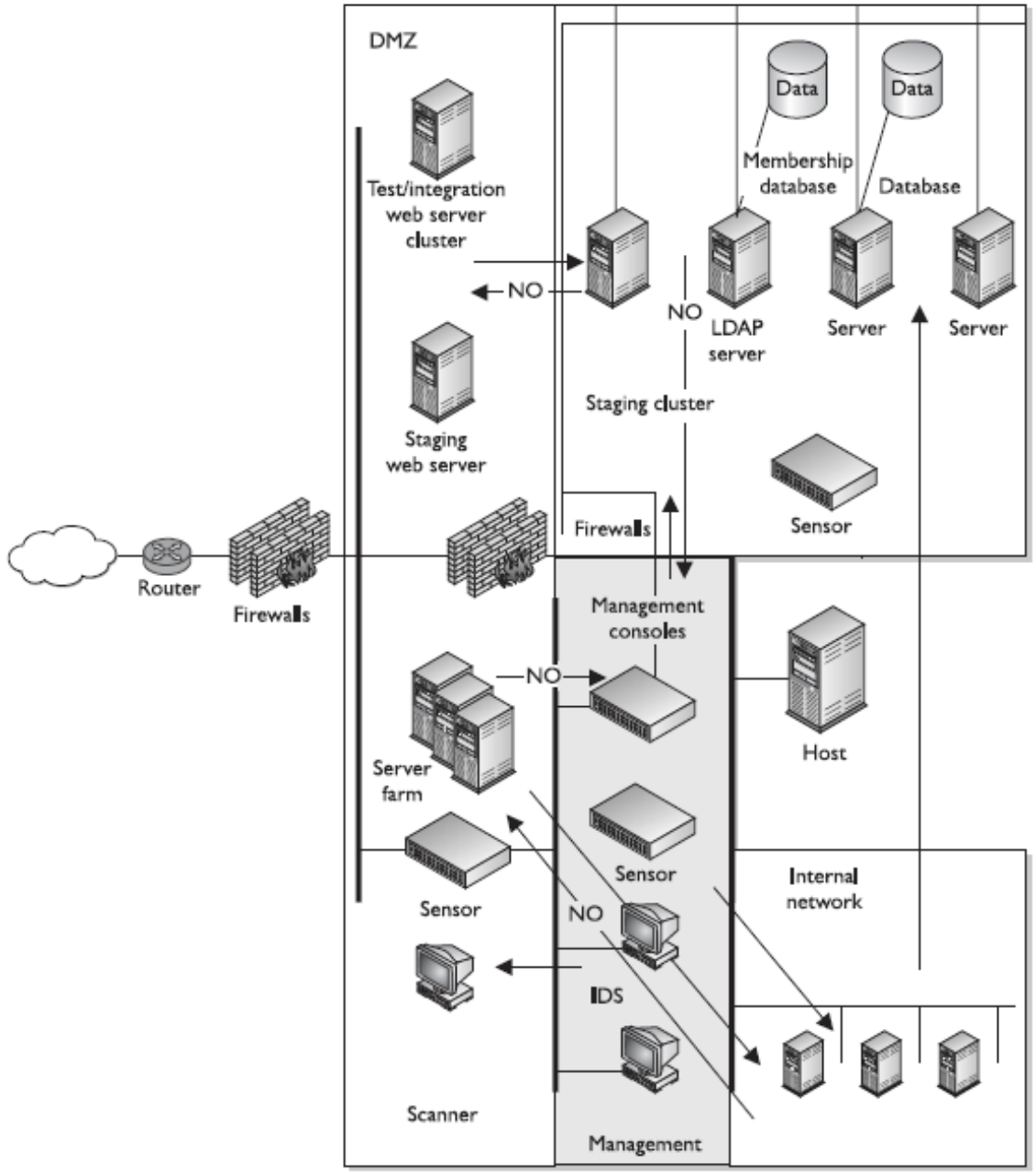


QUEEN'S UNIVERSITY BELFAST

Example Network Models (2)

Another enterprise example:

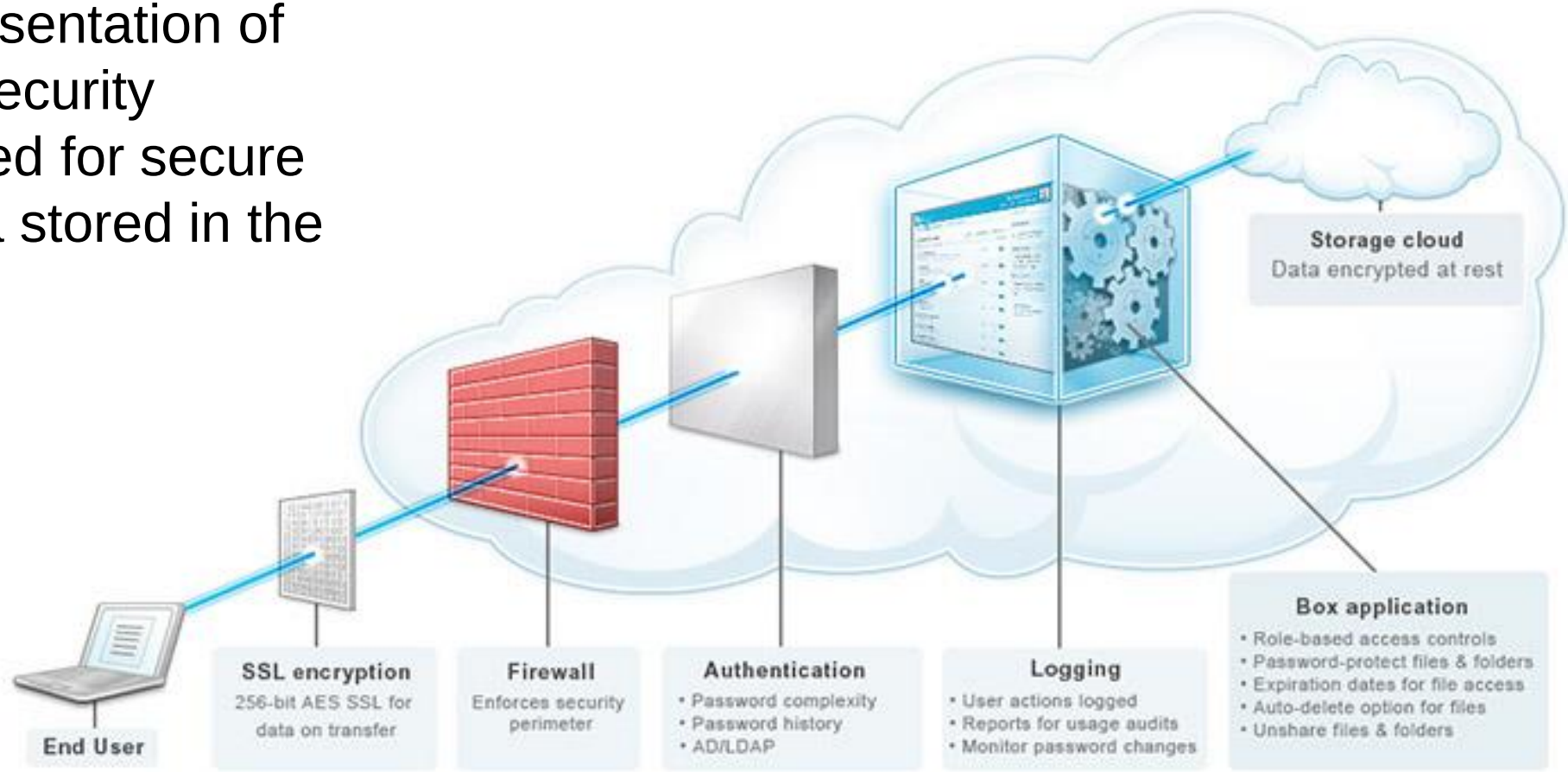
Identify the different security services. We'll be looking at these individually during this course.



QUEEN'S UNIVERSITY BELFAST

Example Network Models (3)

This is a representation of the series of security services applied for secure access to data stored in the cloud.



QUEEN'S UNIVERSITY BELFAST

Summary

- 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 practical model of networked computing, which distinguishes four different levels at 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

QUEEN'S UNIVERSITY BELFAST

Questions?

Next Session: Network Security Architecture – Part 2

Thursday, 24 January 2019

QUEEN'S UNIVERSITY BELFAST