16-124-836
Marcel Matti ZAUDER

8.2 Question 2

8.2.A Provide quick definitions for the following IPsec terms:

Authentication Header Protocol

The Authentication Header provides the message to have the RFC 4302 authentication. However, as of today it is deprecated and should only be used in order to make IPsecv3 backward compatible. For other purposes its use should be discontinued.

Encapsulating Security Payload

A message consisting of an encapsulating header and a trailer which is used in order to provide encryption and authentication in the means of RFC 4303.

Security Association

A security association is defined as the establishment of shared security attributes between two network entities in order to provide the possibility of secure communication.

Security Association Database

The database contains parameters associated with each SA, like Security paramter index, ESP information, the SA's lifetime, the IPsec protocol mode, and others.

Security Policy Database

Is used to map an IP packet to a specific Security Association. This is done within the database with so-called selectors. It can occur that within a database many entries relate to the same SA or one entry relates to many different SAs.