# Packing and Unpacking IPsec packet

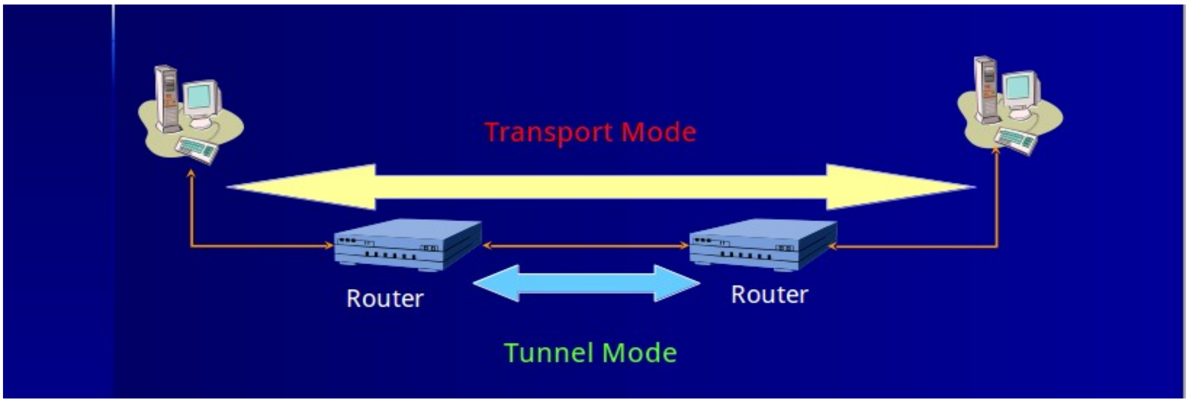
# under transport mode

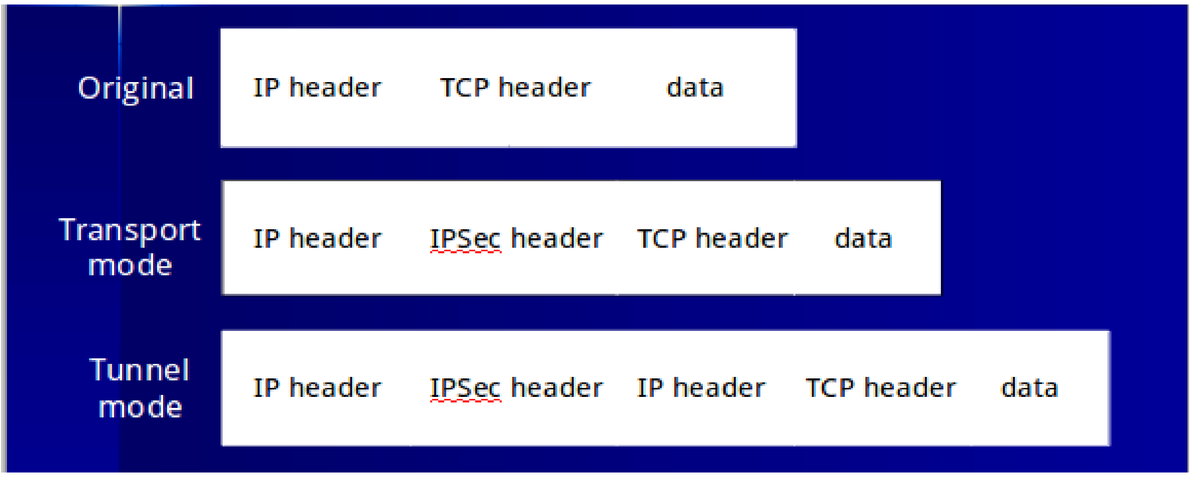
2014-11-6

YiWang ZHENG(12330423)

- Transport mode & Tunnel mode

The different between transport mode and tunnel mode in packing is that the packing method of tunnel mode will handle the whole IP packet with Encapsulated Security Payload(ESP) while in transport mode only the data segment in the level that higher than IP level, such as TCP, UDP data will be handled by ESP.





| | | | | | |
|---|---|---|---|---|---|
| Original | IP header | TCP header | data | | |
| Transport mode | IP header | IPSec header | TCP header | data | |
| Tunnel mode | IP header | IPSec header | IP header | TCP header | data |

- Packing with ESP under transport mode

1. Add ESP trailer

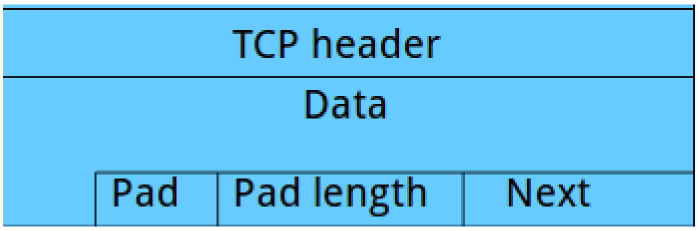
   ESP trailer contains three part: padding, padding length and next header.

Padding - Padding of 0 to 255 bytes is used to ensure that the encrypted payload with the padding bytes are on byte boundaries required by encryption algorithms;

Padding Length - indicates the length of the Padding field in bytes. The receiver uses this field to remove padding bytes after the encrypted payload with the padding bytes has been decrypted

Next Header - Identifies the type of data in the payload, such as TCP or UDP

Packet after add ESP trailer



2. Encrypt the IP payload

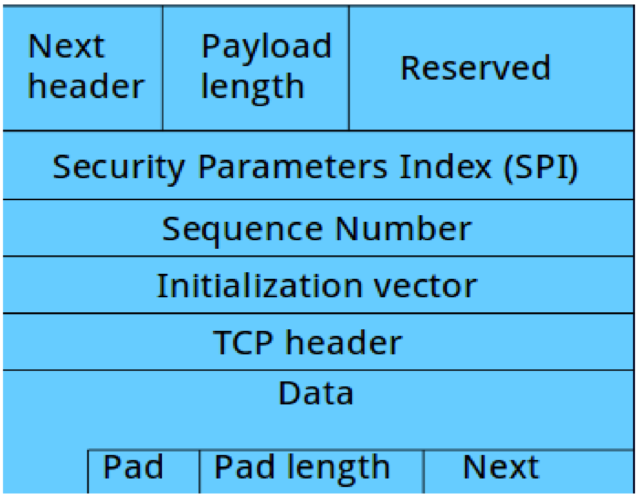
   Encrypt the IP payload (data with out IP header) and ESP trailer with ESP header and add ESP header to the front of the packet.

   - Two important part of ESP header

     Security Parameters Index - Identifies the correct security association for the communication when used in combination with the destination address and the security protocol (AH or ESP). The receiver uses this value to determine the security association with which this packet should be identified

     Sequence Number - Provides anti-replay protection for the packet. The sequence number is a 32-bit, incrementally increasing number (starting from 1) that indicates the packet number sent over the quick mode security association for the communication.

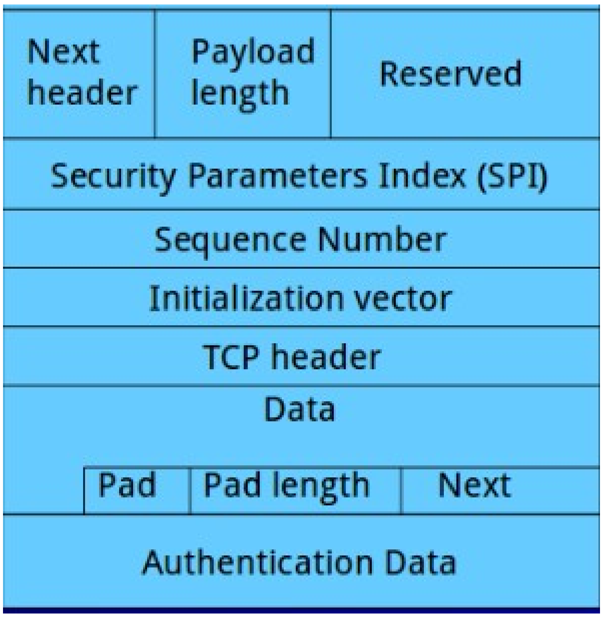
   Packet after add ESP header



3. Add ESP Authentication Data

perform a specific signature algorithm on these three part: ESP header, IP payload and ESP trailer. The result ESP Authentication Data(ESP MAC) will be appended to the end of the packet.

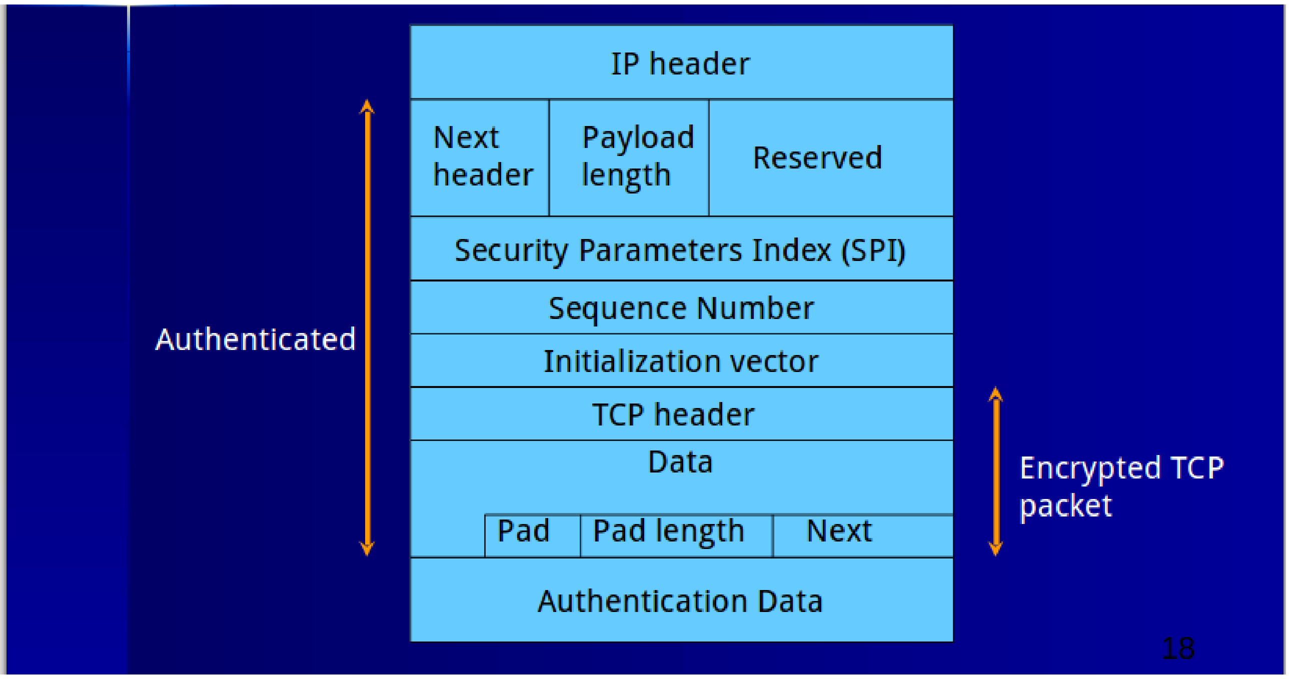
Packet after add authentication data



4. Add the original IP header

add the original IP header to the front of the packet, notice that this IP header is not signed and is not necessarily protected from modification. The protocol type shold be 50 as it's a IPsec packet now.

Result packet



- Unpacking

1. receiver receive a packet and find the protocol type is 50, then know it's a IPsec packet. Use the SPI in the ESP header to determine the corresponding SA.
2. Calculate the message digest of encrypted data, and compare the result with the ESP MAC.
3. Check the sequence number in ESP header to make sure the data is fresh.
4. Use the encryption algorithm and key to decrypt the encrypted data and get the original IP payload with ESP trailer.
5. Remove the padding bit according to the padding length in ESP header and get the original IP payload.
6. Forward the IP payload according to the IP header in the beginning of the received packet.