IPsec
Encryption & Authentication

BİL 448/548

Internet Security Protocols

Ali Aydın Selçuk

IPsec

- Cryptographic protection of the IP traffic, transparent to the user
- Main components:
  - Internet Key Exchange (IKE): IPsec key exchange protocol
  - Authentication Header (AH): Authentication of the IP packet (optional)
  - Encapsulating Security Payload (ESP): Encryption/authentication of the IP packet (optional)

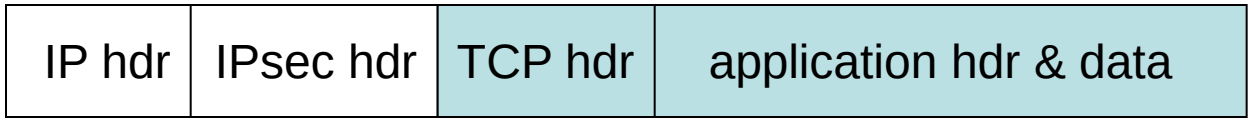
Uses of IPsec

- Can be used to provide user-, host-, or network-level protection (the granularity)
- Protocol modes:
  - Transport mode: Host applies IPsec to transport layer packet
  - Tunnel mode: Gateway applies IPsec to the IP packet of a host from the network (IP in IP tunnel)
- Typical uses:
  - Remote access to network (host-to-gateway)
  - Virtual private networks (gateway-to-gateway)

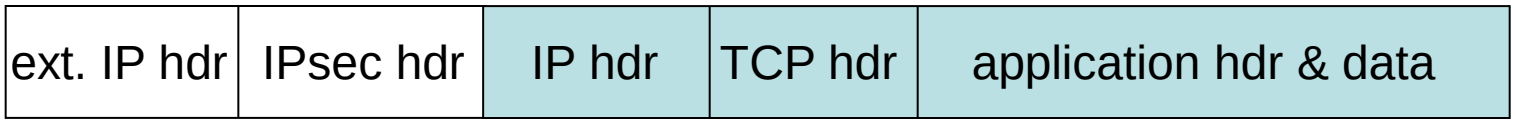
IPsec Coverage

Basic TCP/IP packet:

IPsec – transport mode:



IPsec – tunnel mode:



Some Basics

- Packets are authenticated/encrypted with a session key. Ideally, both parties should contribute to the session key.
- Sequence numbers are needed against packet replay attacks (different from TCP seq.no.).
- Receiver of a packet compares its seq.no. against previous packets in a “sliding window”.
- Session key is reset before seq.no. wraps around.

Security Association & Policy

- *Security Policy Database*

  Specifies what kind of protection should be applied to packets (according to source-destination addresses, port numbers, etc.)
- *"Security Association" (SA)*
  - An IPsec-protected connection
  - Identified by
    - "security parameter index" (SPI)
    - destination IP address
    - protocol identifier (AH or ESP)
  - Specifies the encryption/auth. algorithm, key, etc.

SA Database

Contains the relevant information for each SA:

- AH information (auth. algorithm, key, key lifetime, etc.)
- ESP information (auth./encryption algorithm, key, key lifetime, etc.)
- Sequence number counter
- Anti-replay window (at the destination SA)
- Lifetime of the SA
- Others (protocol mode, path MTU, etc.)

IPsec Packet Processing

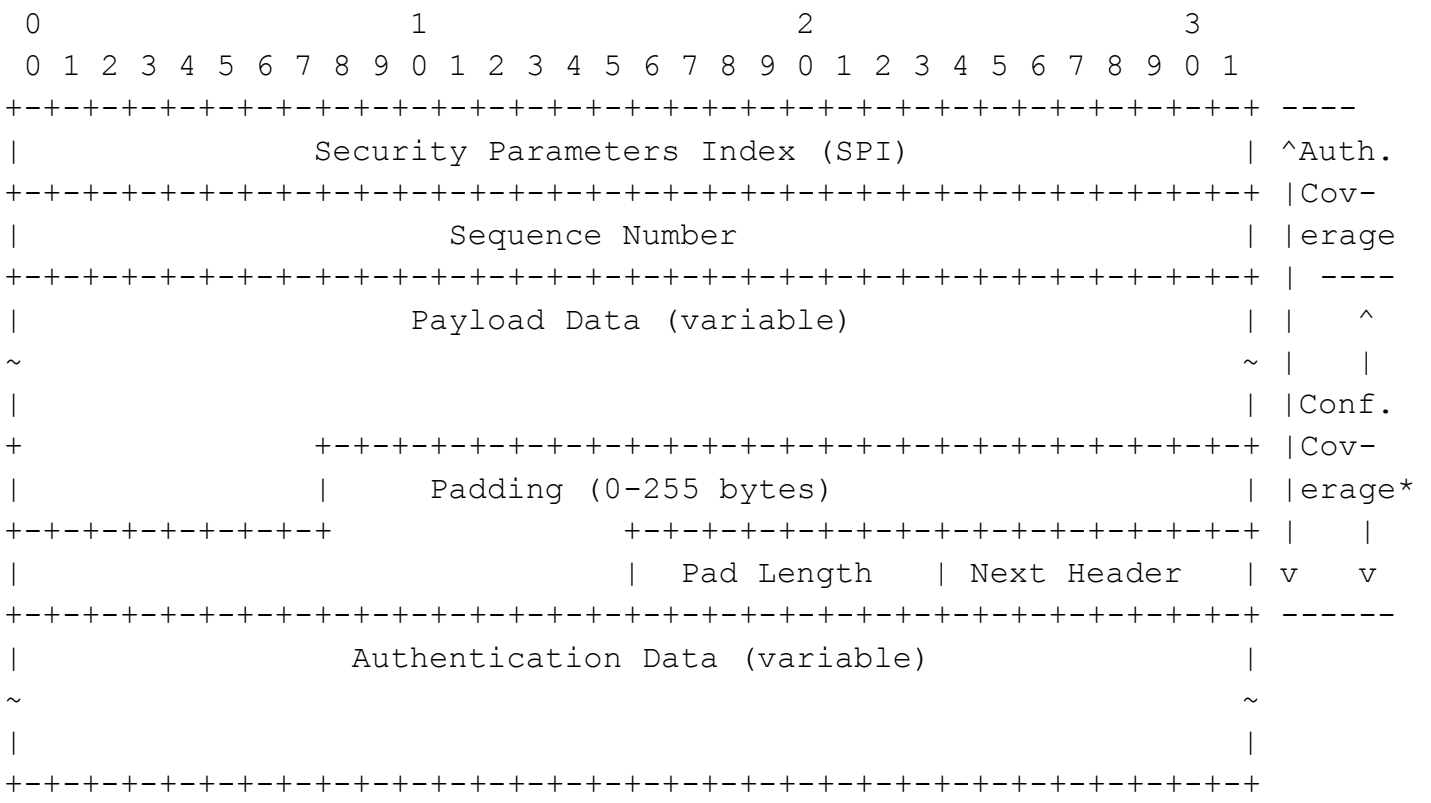
Outbound packets:

- The proper SA is chosen from the security policy database
- From the SA database, the SPI and SA parameters are retrieved
- The IPsec protection is performed; packet passed to IP

Inbound packets:

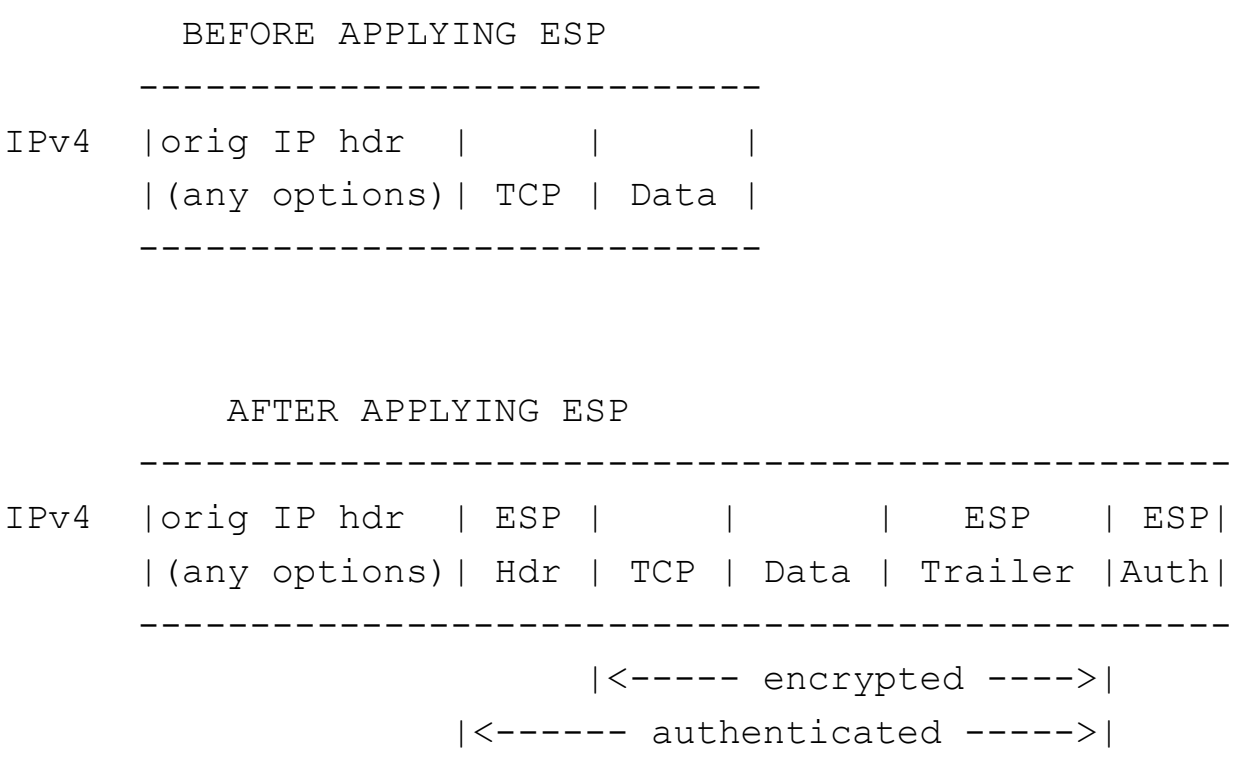
- By the SPI, the SA is found
- IPsec auth./decryption is performed
- Packet passed to upper layer protocol

Encapsulating Security Payload (ESP)

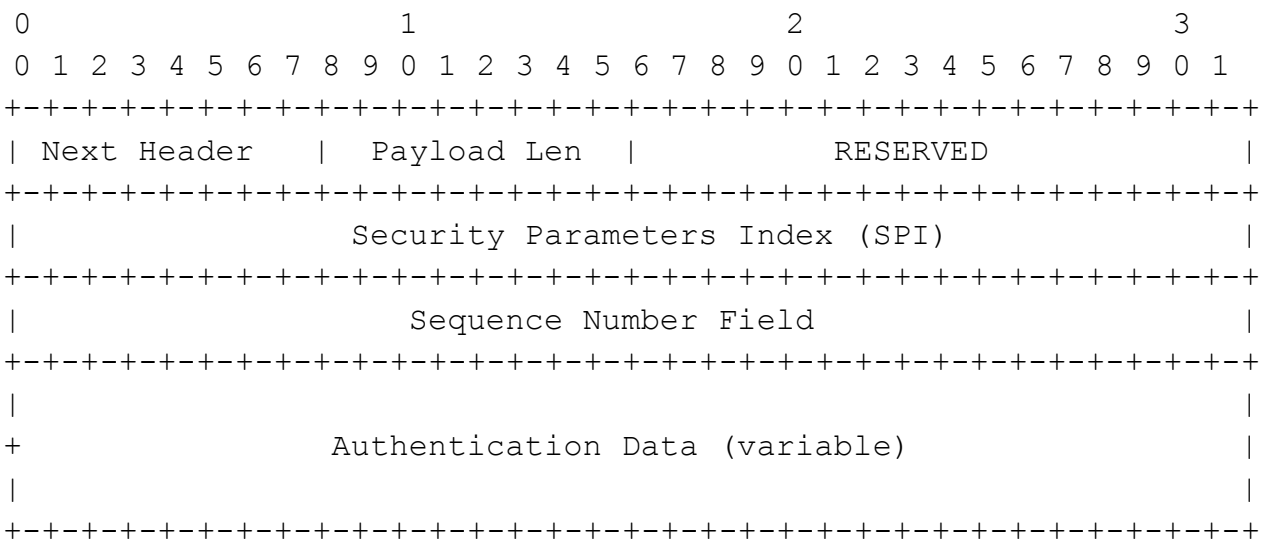


- Encryption: usually a block cipher in CBC mode
- IV is typically included in the payload (not encrypted)

ESP with IPv4

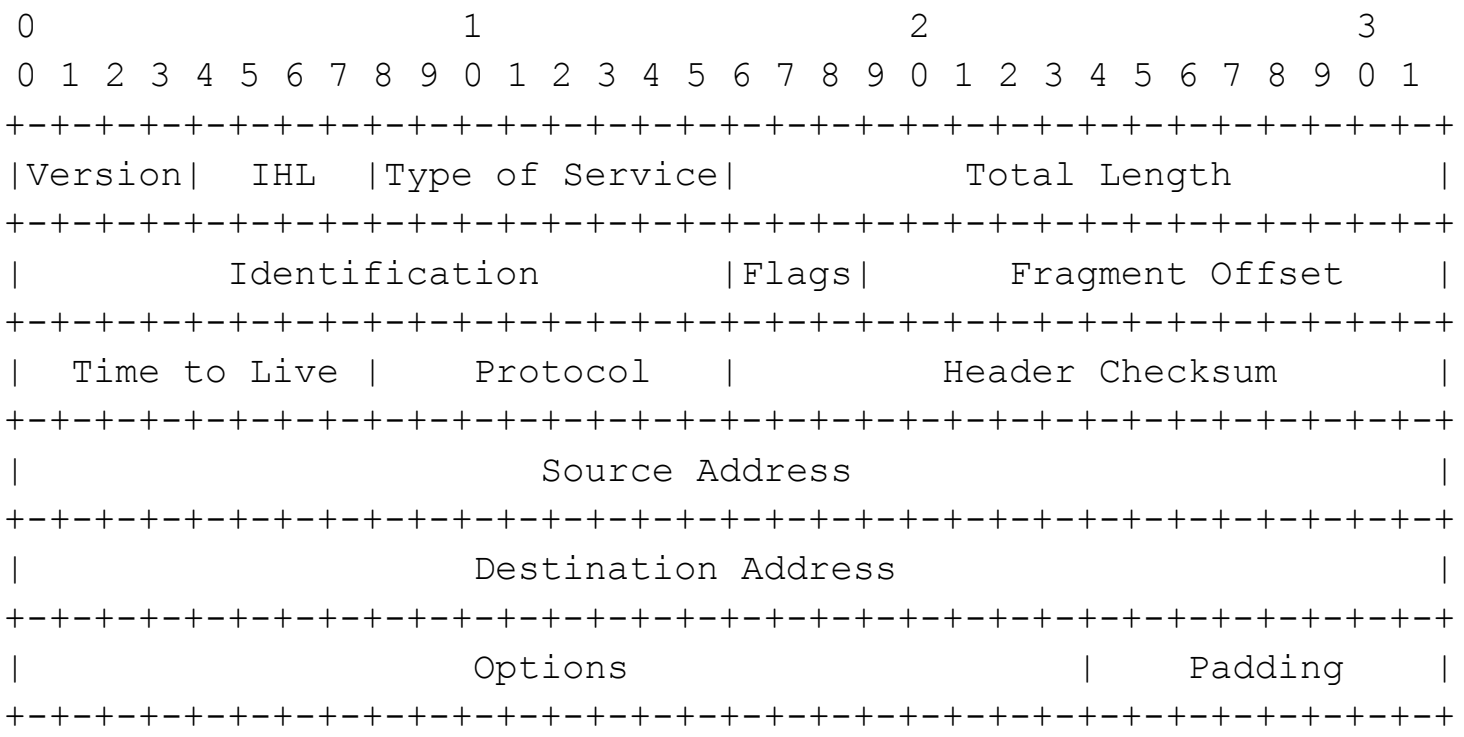


Authentication Header (AH)



- Auth. alg.: HMAC (with MD5, SHA1, etc.)
  CBC-MAC (3DES, RC5, AES, etc.)
- Authentication covers immutable fields of IP header as well as the payload.

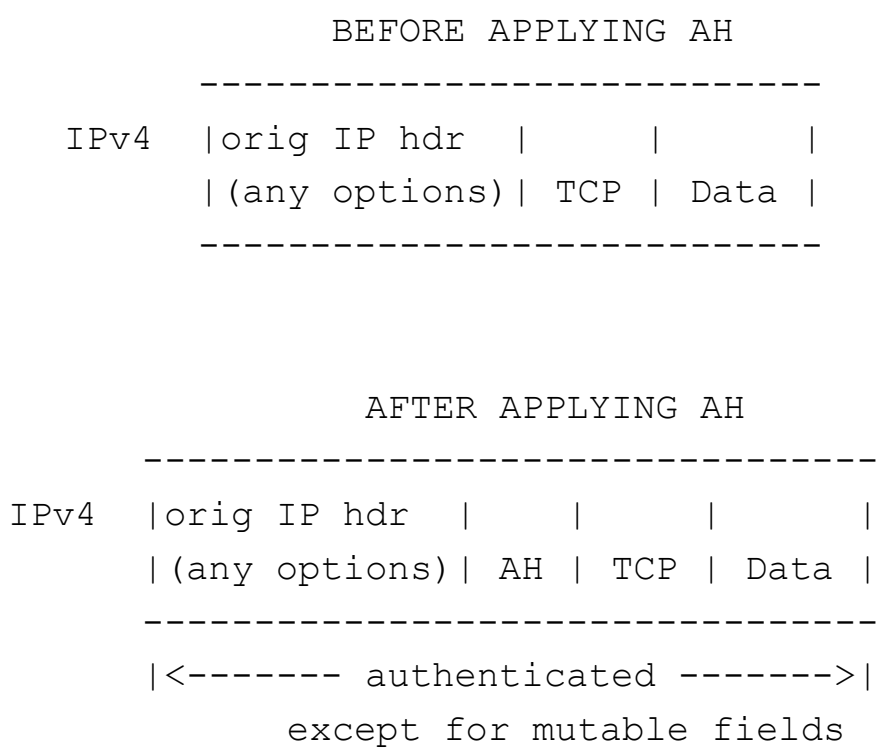
IPv4 Header



Mutable fields (according to AH):

ToS, flags, frag.offset, TTL, checksum

AH with IPv4


BEFORE APPLYING AH
IPv4
orig IP hdr
(any options)
TCP
Data
AFTER APPLYING AH
IPv4
orig IP hdr
(any options)
AH
TCP
Data
authenticated
except for mutable fields

AH Controversies

- Authentication is provided by ESP as well (hence, AH is useless)
- Protecting immutable fields doesn’t add much
- Destination address may be mutable! (due to NAT)
- Not efficient to compute (MAC at the beginning)