CSCI 7000-001 — Network-level Security: IPSec Basic Architecture, AH, and ESP

October 23, 2001

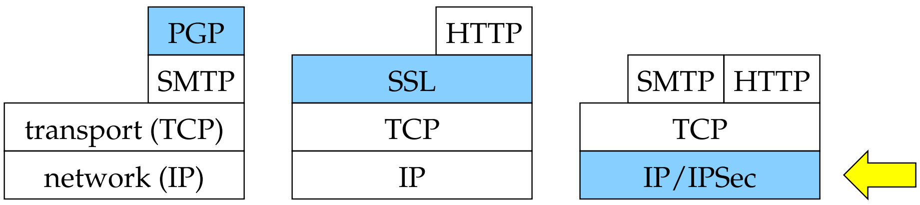
References:

- RFC 2401 (`http://www.ietf.org/rfc/rfc2401.txt`)

1 IP-level security overview: goals

IPsec is designed to provide interoperable, high quality, cryptographically-based security for IPv4 and IPv6. In particular:

- access control
- connectionless integrity
- data origin authentication
- protection against replays (a form of partial sequence integrity)
- confidentiality (encryption)
- limited traffic flow confidentiality.



These services are provided at the IP layer, offering protection for IP and/or upper layer protocols.

2 General benefits of IPSec

- network-,transport-, and application-level
  - virtual private networks
  - transparent security for applications and users
- routing infrastructure
  - authentication for routing advertisements

3 How IPSec applies to network traffic

- applications are oblivious to the IPSec
- so who decides where, when, and how to apply security?

For each packet, an IPSec implementation decides whether to

- discard that packet
- bypass IPSec security services, or
- afford IPSec security services

In other words, applying IPSec security services is largely a network management decision.

4 Security Policy Database (SPD)

The decision is based on a *security policy*, stored in a Security Policy Database (SPD).
The SPD contains an ordered list of policy entries. Each entry is defined by one or more *selectors*, and an indication whether the traffic matching this policy will be bypassed, discarded, or subject to IPsec processing.

- source address
- destination address
- protocol (IPv4 Protocol or IPv6 Next Header field)
- source port
- destination port
- user id
- ...

Selectors may use single values, lists of values, or wild-card expressions.

5 How IPSec provides security

IPsec uses two protocols to provide traffic security:

- *Authentication Header (AH)* provides connectionless integrity, data origin authentication, and an optional anti-replay service.
- *Encapsulating Security Payload (ESP)* provides
  - confidentiality (encryption), and limited traffic flow confidentiality, and optionally
  - data origin authentication, and an anti-replay service

Both AH and ESP, indirectly, provide access control, based on the distribution of cryptographic keys and the management of traffic flows relative to these security protocols.

6 Summary of mapping of services to protocols

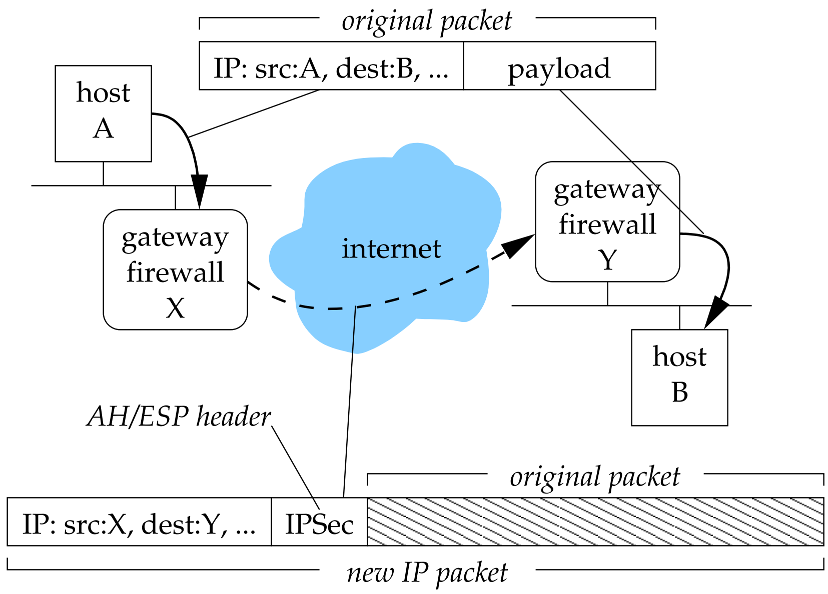
	AH	ESP authentication	ESP authentication + encryption
access control	•	•	•
connectionless integrity	•		•
data origin authentication	•		•
rejection or replayed packets	•	•	•
confidentiality		•	•
limited traffic flow confidentiality		•	•

7 Transport and tunnel modes

Both AH and ESP can function in either

- *transport mode* provides security for upper-level protocols (such as TCP or UDP) by authenticating and/or encrypting the payload
- *tunnel mode* provides security for the whole IP packet by encapsulating (tunneling) that packet into another IP packet.

8 Virtual private networks with tunnel mode



9 Security associations (SA)

- key concept appearing in both authentication and confidentiality mechanisms of IPSec
- *one-way* relation
- between a *sender* and a *receiver*

a security association is identified by

- *security parameter index (SPI)*: a key that identifies a set of parameters for this association, stored in the Security Association Database
- *destination address* (currently only unicast addresses)
- *security protocol identifier*: AH or ESP

10 Authentication Header (AH)

0	8	16 31
next header	payload len	reserved
security parameters index (SPI)		
sequence number		
authentication data (variable)		

- integrity of some header fields ⇔ authentication
- protection against replay attacks

11 Authentication data in AH

Authentication data contains the MAC for the packet. It is a *variable-length* field. The current specification mentions two MAC algorithms:

- HMAC-MD5-96
- HMAC-SHA-1-96

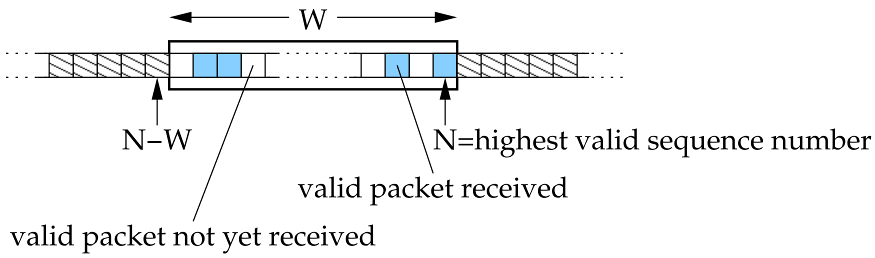
The value of *authentication data* (MAC) is computed over

- immutable IP header fields, for example:
  - IPv4 Internet Header Length
  - IPv6 Version
  - Source Address
- predictable IP header fields, for example:
  - destination address
- AH header (other than Authentication Data field)
- the entire payload (which is immutable in transit)

Mutable fields are zeroed when computing the MAC.

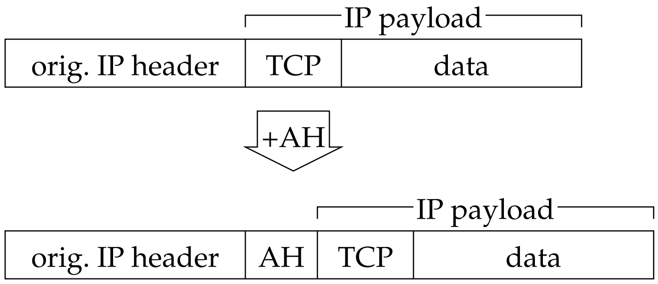
12 Protection against replay attacks in AH

The Sequence Number field allows some protection against replay attacks. If this feature is enabled, the sender must make sure that Sequence Number is initialized to 0 and incremented for each packet sent over the same SA.
IP is unreliable, therefore the receiver must keep track of what sequence number it has seen. The specification mandates a window of fixed size W (default $W = 64$)



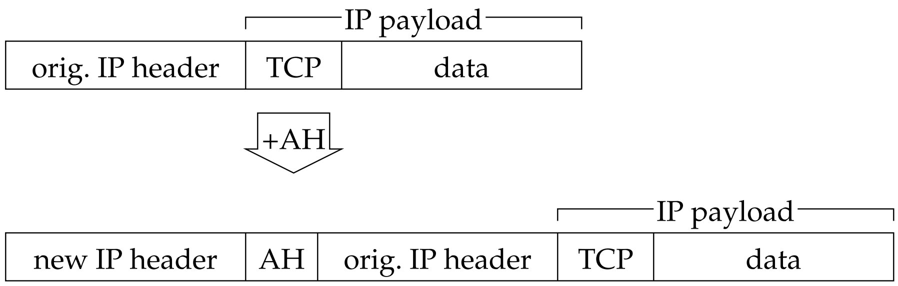
13 Transport mode for AH

For *transport mode AH*, the authentication header is inserted after the original IP header and before the IP payload (with some minor differences between IPv4 and IPv6):

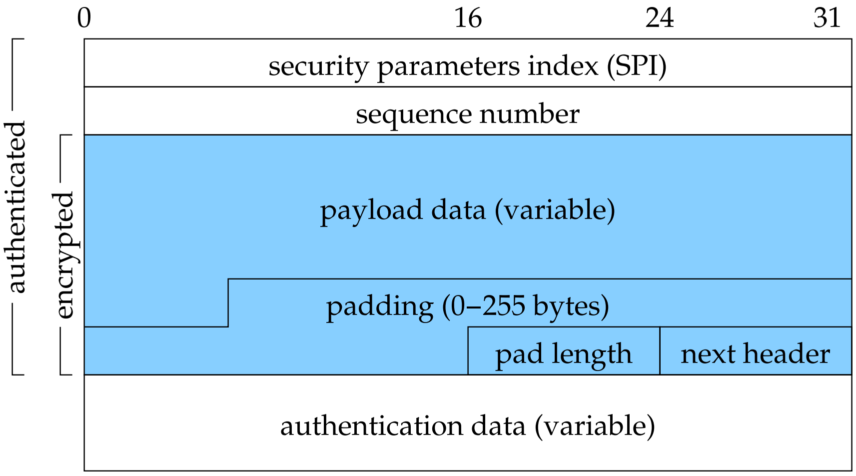


14 Tunnel mode for AH

For *tunnel mode AH*, the original IP packet is encapsulated within another IP packet. The authentication header authenticates the entire original IP packet, and is inserted between the outer IP header and the inner (original) IP header.



15 Encapsulating Security Payload (ESP)



- confidentiality of payload
- integrity (⇔ authentication)
- protection against replay attacks

16 Authentication and reply attack protection in ESP

- *protection against replay attack*: same as in AH
  - sender manages Sequence Number
  - receiver implements sliding window
- *integrity and authentication*: computed over ESP header (SPI and Sequence Number)

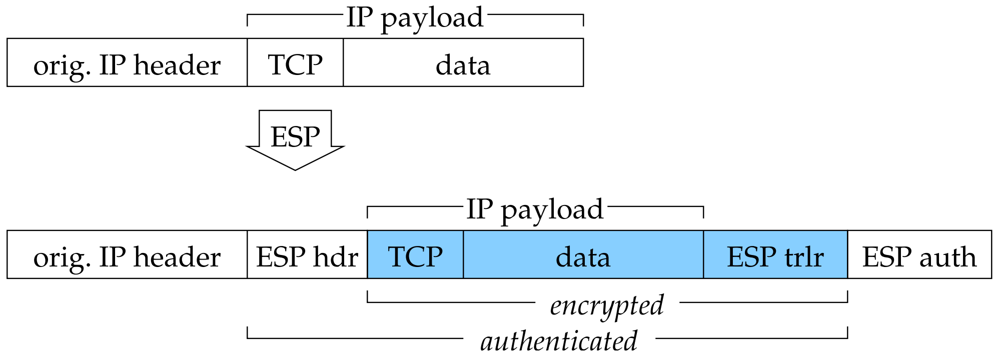
17 Confidentiality in ESP

- covers payload
- padding
  - match plaintext length required by encryption algorithm
  - additional confidentiality, by hiding the actual payload length
- *encryption algorithm*: implementations must support DES in CBC
- other algorithms have been identified:
  - 3DES

- RC5
- IDEA
- 3IDEA
- CAST
- Blowfish

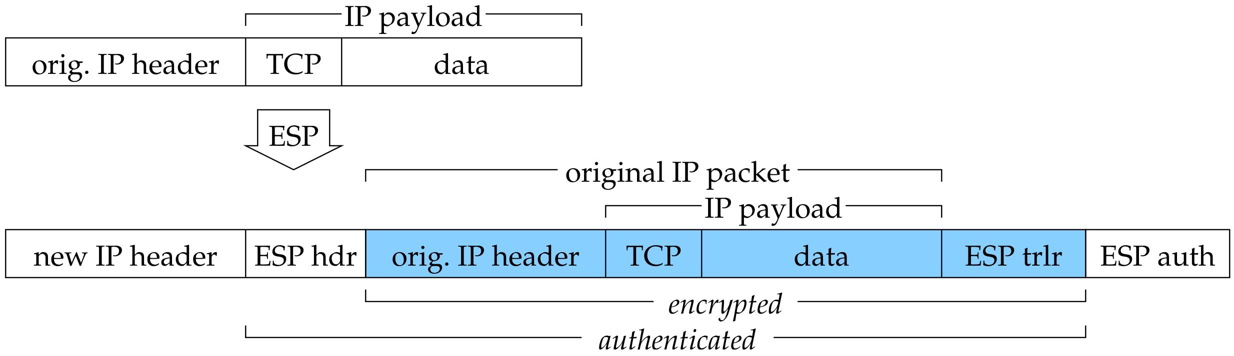
18 Transport mode for ESP

Transport mode ESP can be seen as a simple IP payload: the ESP packet is inserted after the original IP header (with some minor differences between IPv4 and IPv6):



19 Tunnel mode for ESP

For *tunnel mode ESP*, the original IP packet is encapsulated within another IP packet as an encrypted and (optionally) authenticated ESP:



20 Security associations parameters

Here's what a SA stores:

- *sequence number counter*: 32-bit value used to generate sequence numbers in AH and ESP headers
- *sequence counter overflow*: flag indicating whether an overflow of the sequence number counter should produce an auditable event
- *anti-replay window*
- *AH information*: authentication algorithm, keys, key lifetime, other AH-related parameters
- *ESP information*: encryption and authentication algorithms, keys (encryption, and auth.), key lifetimes, initialization values, and other ESP-related parameters
- *lifetime of the SA* time interval or byte count after which an SA must be replaced with a new SA (and new SPI) or terminated
- *IPSec protocol mode*
- *path MTU*

21 Some comments

- key exchange and cipher negotiation is outside the scope of the basic architecture
- policy definition is outside of the scope of IPSec
- policy implementation is essentially a network management issue
- tunneling modes, especially in ESP with authentication allows you to set up virtual private networks
- transport mode provides a security service comparable to transport-level security