Building the IPsec Protocol

Joe Abraham
NETWORK SECURITY CONSULTANT
@joeabrah www.joeabrahamtech.com

Overview

IPsec building blocks

IPsec components

SA establishment protocols

IPsec demonstration

“With a bucket of Lego, you can tell any story. You can build an airplane or a dragon or a pirate ship - it's whatever you can imagine.”

Christopher Miller

IPsec Protocol Suite

Security Protocols

Security Associations

Building Blocks

Key Management

Cryptographic Algorithms

IPsec Building Blocks

AH and ESP

Authentication Header (AH)

Data integrity

Authentication

Anti-replay

Access control

Protocol number 51

Encapsulating Security Payload (ESP)

Data integrity

Authentication

Anti-replay

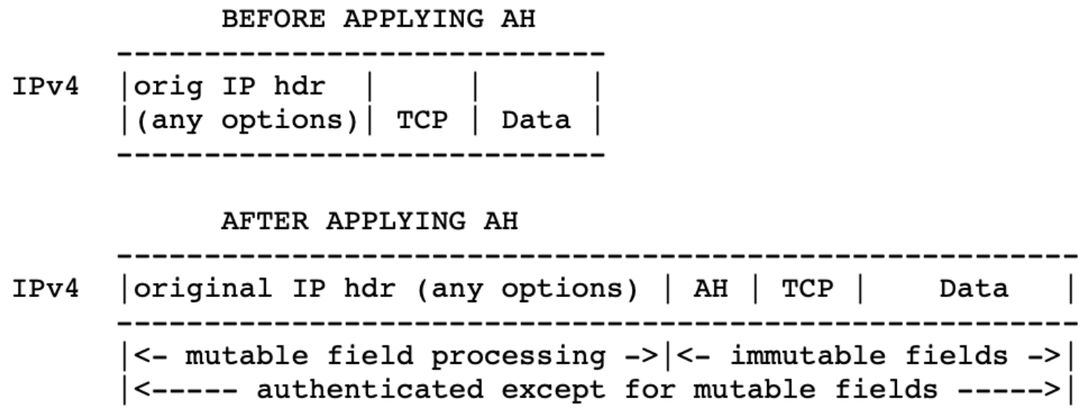
Confidentiality

Access control

Protocol number 50

AH Transport and Tunnel Modes

Transport Mode



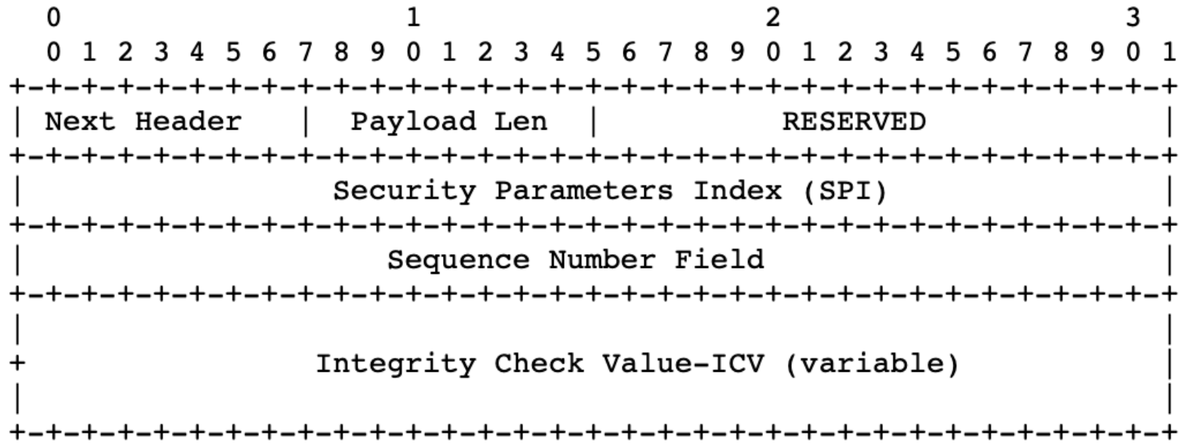
Next Header: 1 byte

Payload Length: 1 byte

SPI: 4 bytes

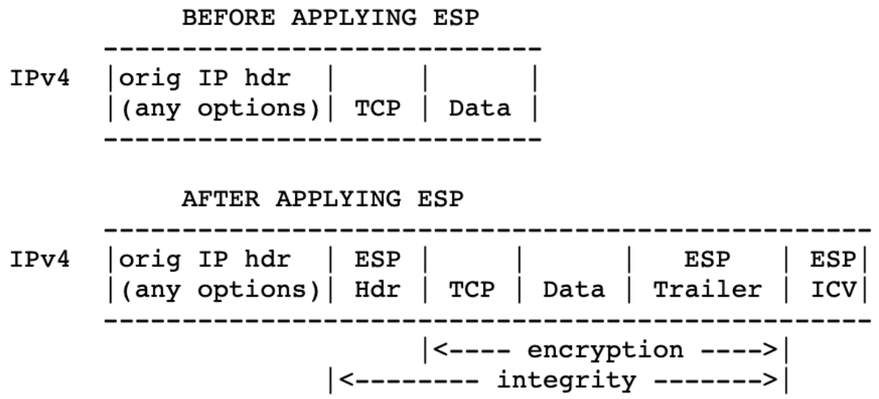
Sequence Number: 4 bytes

ICV: variable bytes

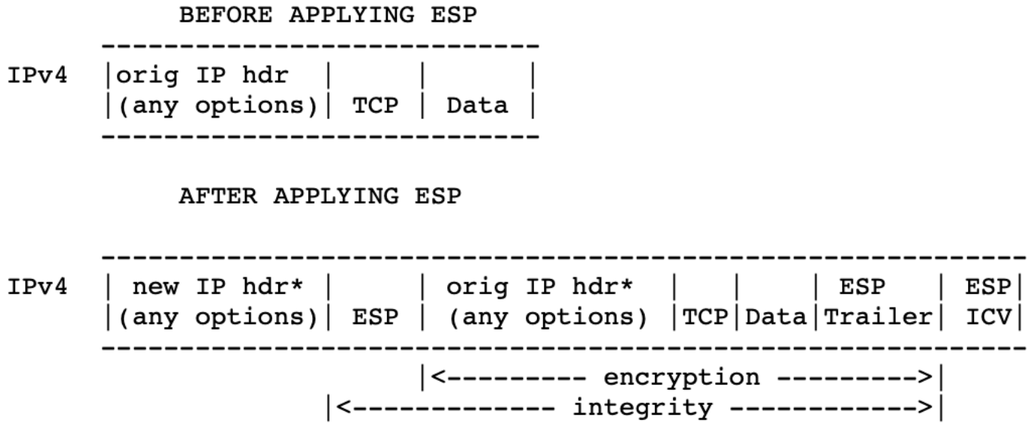


ESP Transport and Tunnel Modes

Transport Mode



Tunnel Mode



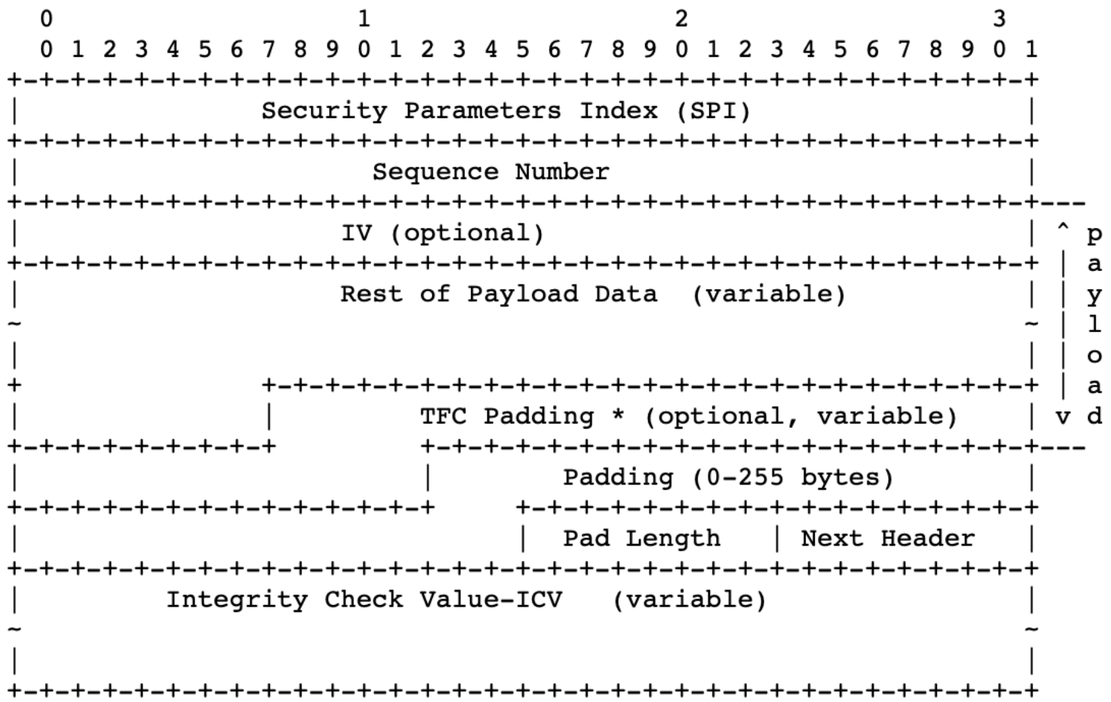
No next header!

No payload length!

SPI: 4 bytes

Sequence Number: 4 bytes

ICV: variable bytes in trailer



Security Association

Unidirectional connections

- Need a pair for bidirectional communication
- SPI, destination IP address, and security protocol

Key Management

Automated

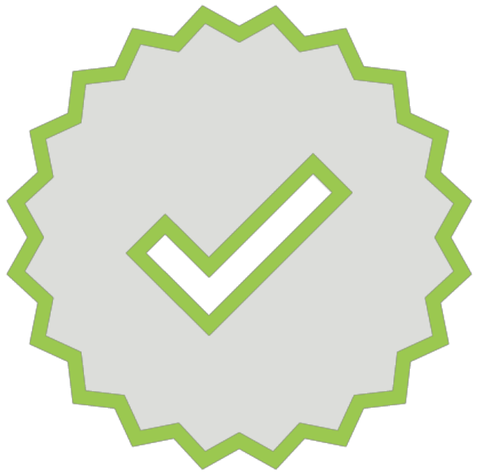
(IKEv1 and IKEv2)

Manual

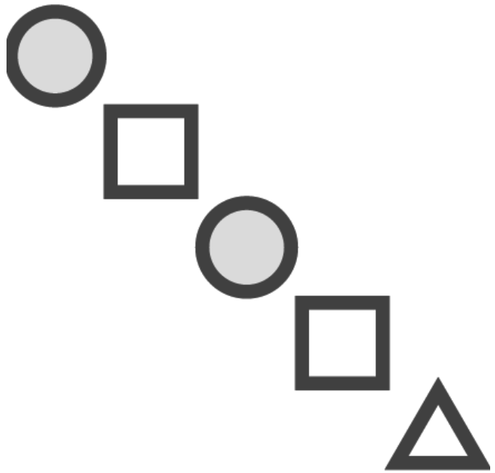
Cryptographic Algorithms

Encryption

Authentication



Integrity



Pseudorandom Function

IPsec Components

SPI

A 32-bit value that identifies the SA

SPD

Holds IPsec service information (what and how)

SAD

SA parameters, SPI, lifetime, etc.

PAD

Links the SPD and SA management protocol

SA lifetime can be either time-based or usage-based.

SA Establishment Protocols

ISAKMP

Internet Security Association and Key Management Protocol. Used for procedures and formats to establish SAs.

OAKLEY and SKEME

OAKLEY gives us key exchange mechanisms. Used to exchange key material over insecure connections using Diffie-Hellman

SKEME gives anonymity and reputability through key exchange techniques

IKE uses a combination of ISAKMP, OAKLEY, and SKEME!

Demo

Look at VPN link packets without IPsec

Look at VPN link packets with IPsec

CLI deep dive into IPsec components

Summary

IPsec building blocks

IPsec components

SA establishment protocols

IPsec demonstration