ESP Header Compression Profile

draft-ietf-ipsecme-diet-esp

Authors:

Migault, Hatami, Cespedes, Atwood, Guggemos, Bormann, Schinazi

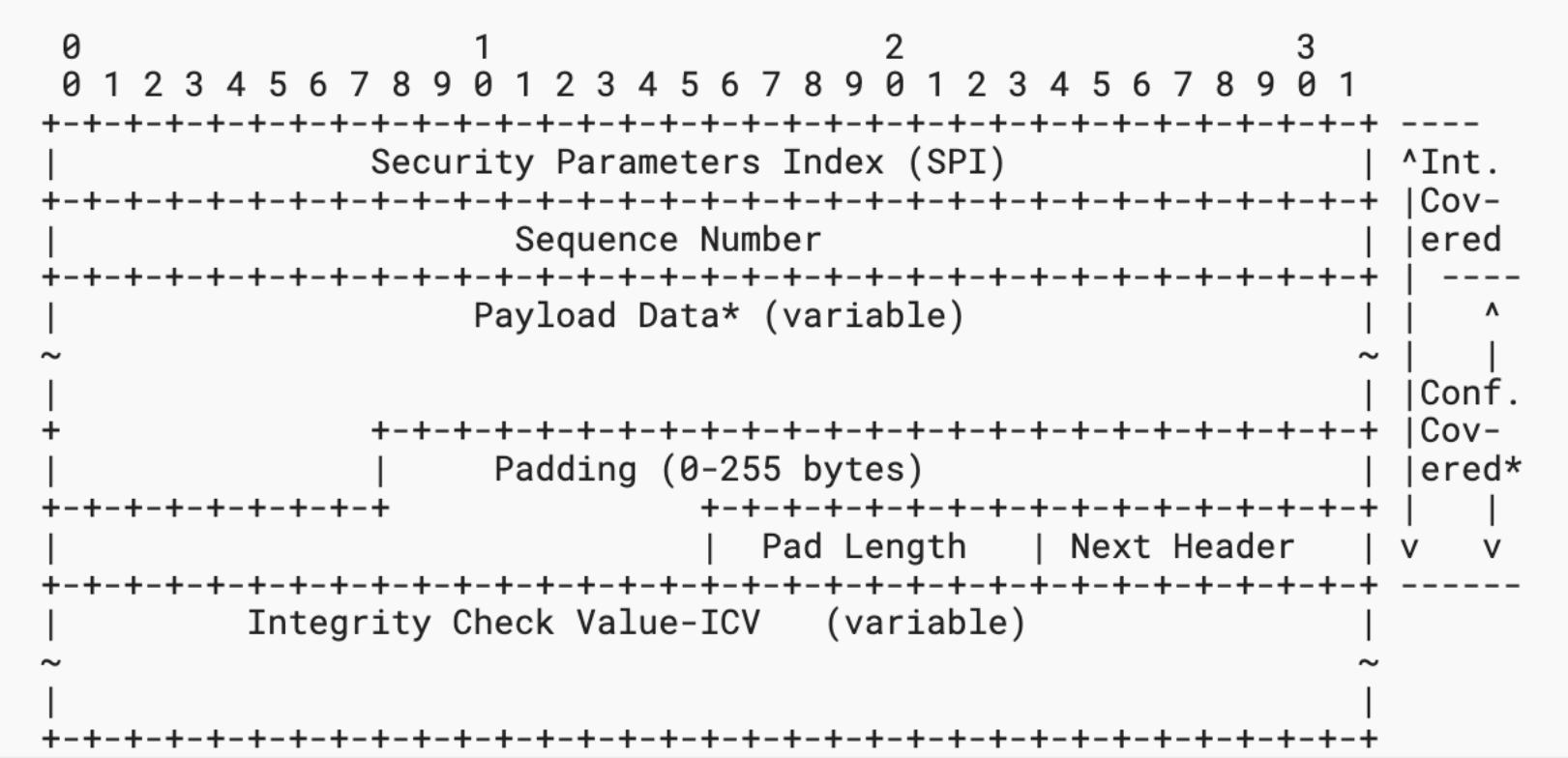
IETF 120, Vancouver, 26 July 2024

Introduction

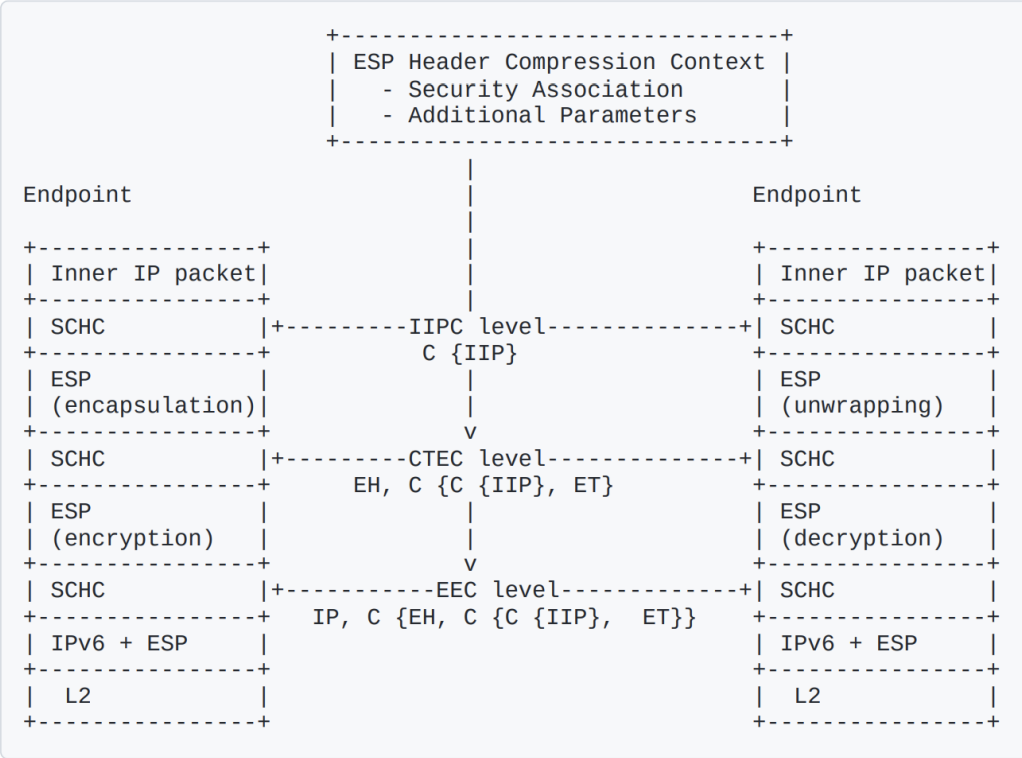
This document defines the ESP Header Compression profile (EHCP) for compression/decompression of IPsec Encapsulating Security Payload (ESP) packets using SCHC.

This is a joint work with the ipsecme WG.

ESP Packet Structure



Levels of Compression

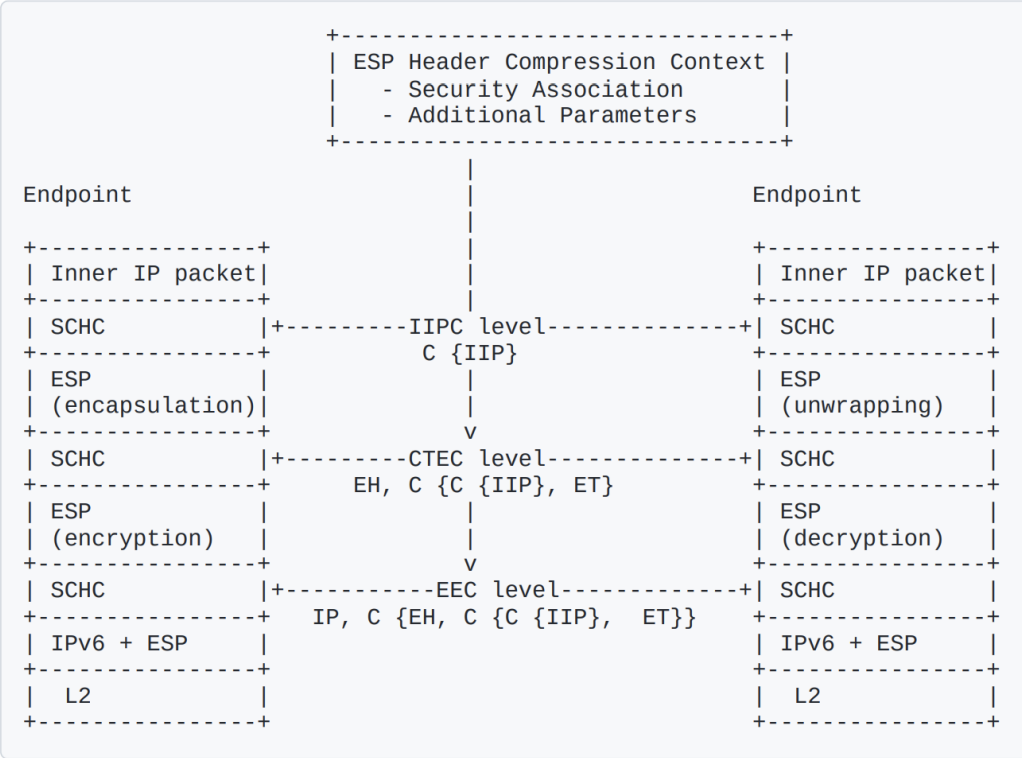


1. Inner IP Compression (IIPC)

2. Clear Text ESP Compression (CTEC)

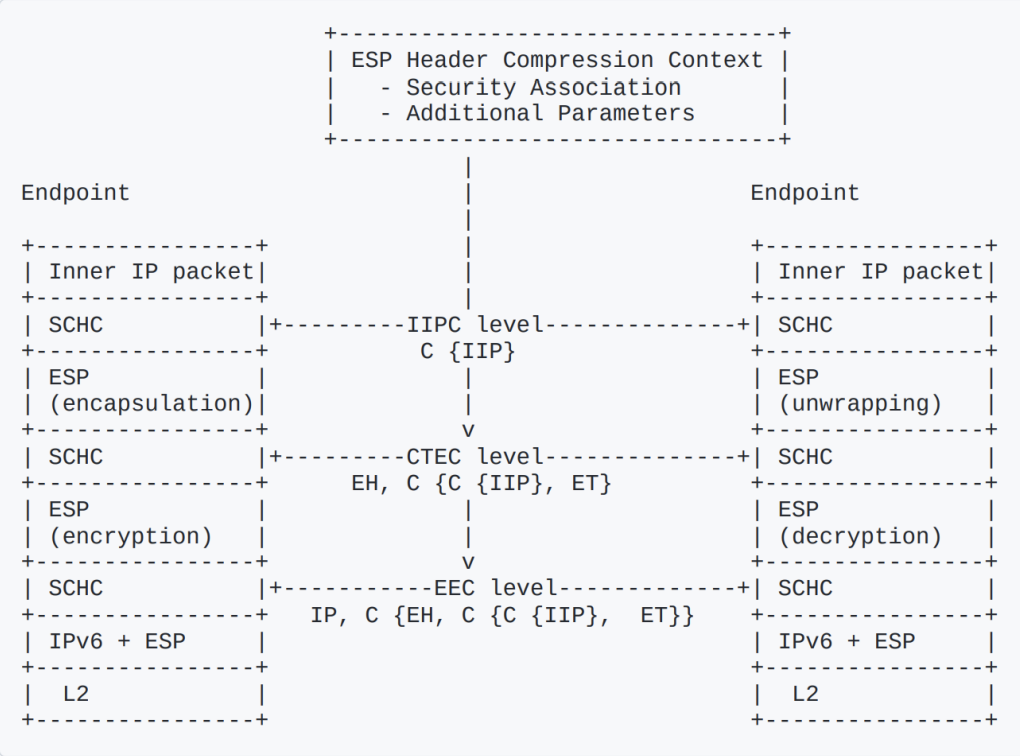
3. Encrypted ESP Compression (EEC)

Inner IP Compression (IIPC)



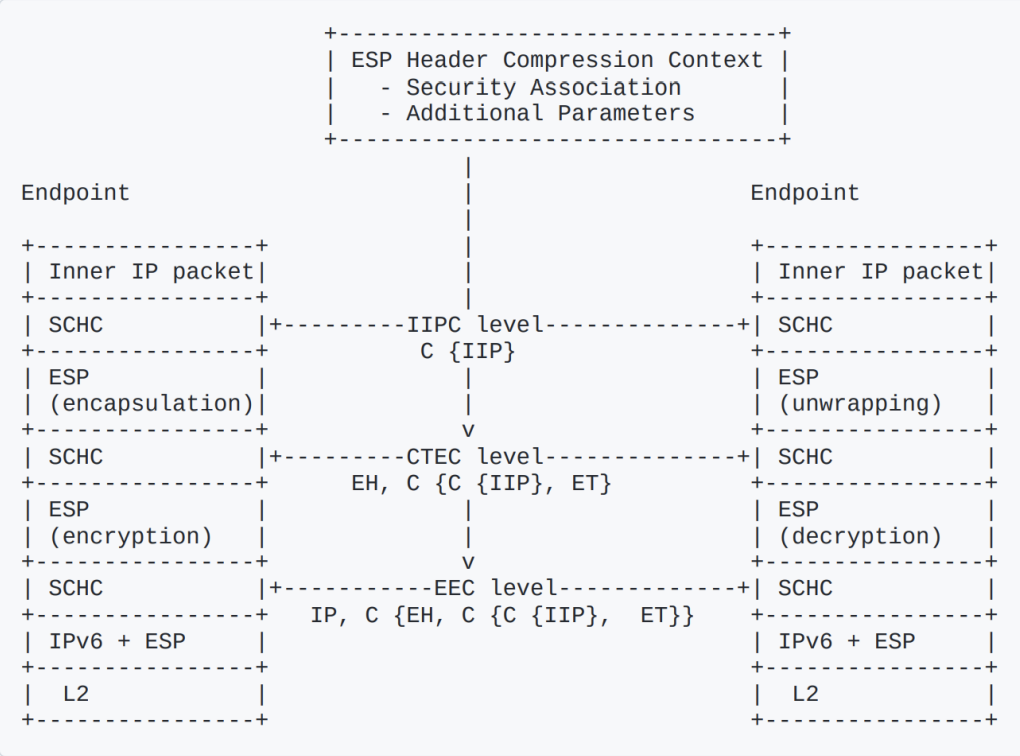
- Happens directly on the inner IP packet.
- Compresses fields such as UDP ports and checksums.
- If no compression of the inner packet is possible, the resulting SCHC packet contains the uncompressed IP packet.

Clear Text ESP Compression (CTEC)



- Compresses fields of the ESP payload right before being encrypted.

Encrypted ESP Compression (EEC)



- Compresses ESP fields that remain after encryption.
- Typically involves fields such as the Security Parameters Index (SPI) and Sequence Number (SN).

SCHC Parameterization for ESP

Various parameters are considered in the EHCP Context.

Implementations may consider different expressions of the parameters, but their behavior is expected to remain compatible.

EHC Context	Possible Values	Reference	C / D
alignment	"8 bit", "32 bit"	ThisRFC	CTEC
ipsec_mode	"Tunnel", "Transport"	RFC4301	CTEC
tunnel_ip	IPv4, IPv6 address	RFC4301	CTEC
esp_spi	ESP SPI	RFC4301	EEC
esp_spi_lsb	0, 1, 2, 3, 4*	ThisRFC	EEC
esp_sn	ESP Sequence Number	RFC4301	EEC
esp_sn_lsb	0, 1, 2, 3, 4*	ThisRFC	EEC
esp_encr	ESP Encryption Algorithm	RFC4301	CTEC
ts_flow_label	True, False	ThisRFC	CTEC
ts_ip_version	4, 6	ThisRFC	CTEC
ts_ip_src_start	IP4 or IPv6 address	ThisRFC	CTEC
ts_ip_src_end	IP4 or IPv6 address	ThisRFC	CTEC
ts_ip_dst_start	IPv4 or IPv6 address	ThisRFC	CTEC
ts_ip_dst_end	IPv4 or IPv6 address	ThisRFC	CTEC
ts_proto_list	TCP, UDP, ..., 0	ThisRFC	CTEC
ts_port_src_start	Port number	ThisRFC	CTEC
ts_port_src_end	Port number	ThisRFC	CTEC
ts_port_dst_start	Port number	ThisRFC	CTEC
ts_port_dst_end	Port number	ThisRFC	CTEC
ts_dsp_list	DSCP number	RFCYYYY	CTEC

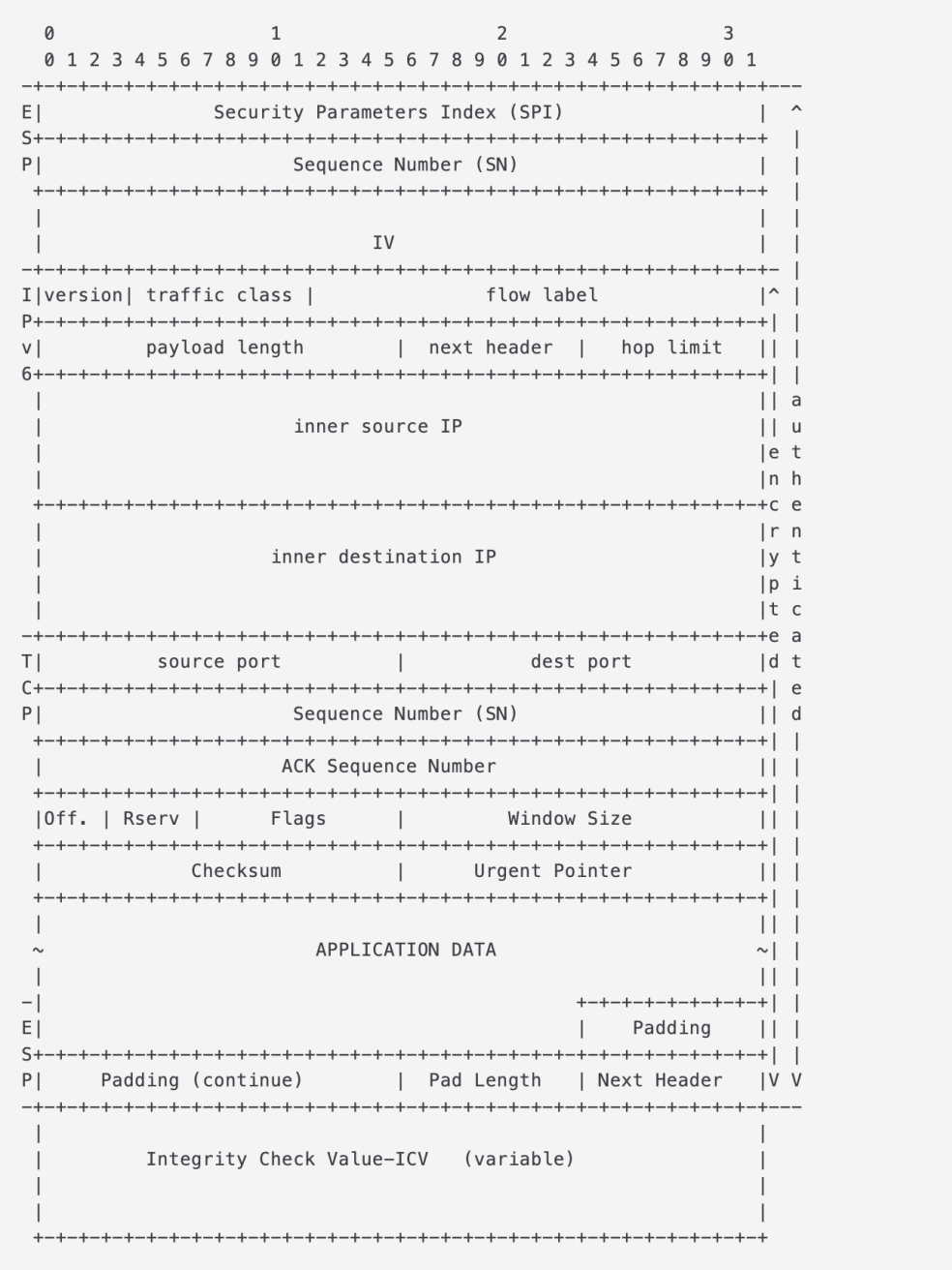
New SCHC CDA

Action	Compression	Decompression
lower	elided	Get from lower layer
checksum	elided	Compute checksum
padding	elided	Compute padding
flow_label	elided	Compute flow label

Introduces new Compression/Decompression Actions (CDA) to use SCHC.

- We define the following CDA and want to check this is the proper way to use SCHC:
- lower indicates that the value is sent in the packet but not at the expected place. In our case, we have IP in IP, and it means the compressed field of the inner packet is read from the outer packet.
- checksum indicates checksum needs to be computed following the specific rules.
- padding indicates padding bits (for ESP) are generated in a certain way.
- flow_label: generates a completely new flow label. The receiving SG generates a NEW flow label.

IPv6 in IPv6 Example



Next Steps

Completing some sections in the document which still needs some work.

The implementation is in progress (The plan is to demo by September 2024)

Questions and Comments?