Wrapped ESP v2

draft-klassert-ipsecme-wespv2-01

Steffen Klassert

Why a new security protocol?

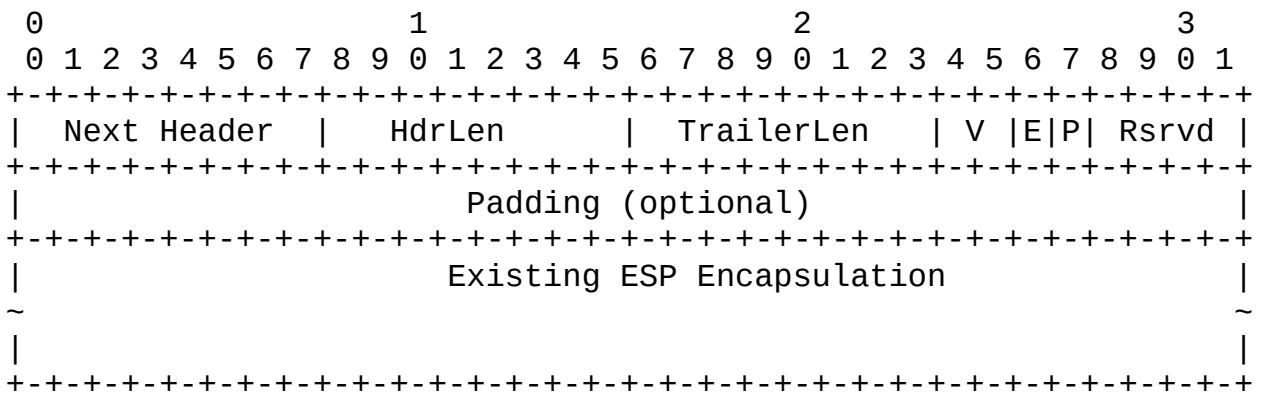
- ESP is unflexible
  - No version number
  - New features must be negotiated
  - Not transparent to the network
- Lot of proposals to extend ESP
  - Suffer from ESP limitations
- Need to be HW offload friendly: Google PSP
  - Similar to ESP but more flexible
  - No standard!

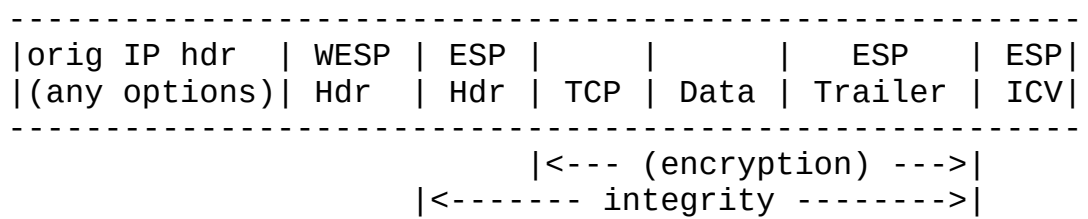
Wrapped ESP (WESP)

WESP

- RFC 5840
- ESP wrapper
- AH replacement
- Has an encryption (E) Flag
    - If set: Packet is authenticated **and** encrypted
    - If not set: Packet is authenticated **but not** encrypted
- Inner packet can be parsed if E is not set
- Has 2 bit version number (version 00 currently)

WESP


0 1 2 3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
Next Header
HdrLen
TrailerLen
V
E
P
Rsrvd
Padding (optional)
Existing ESP Encapsulation

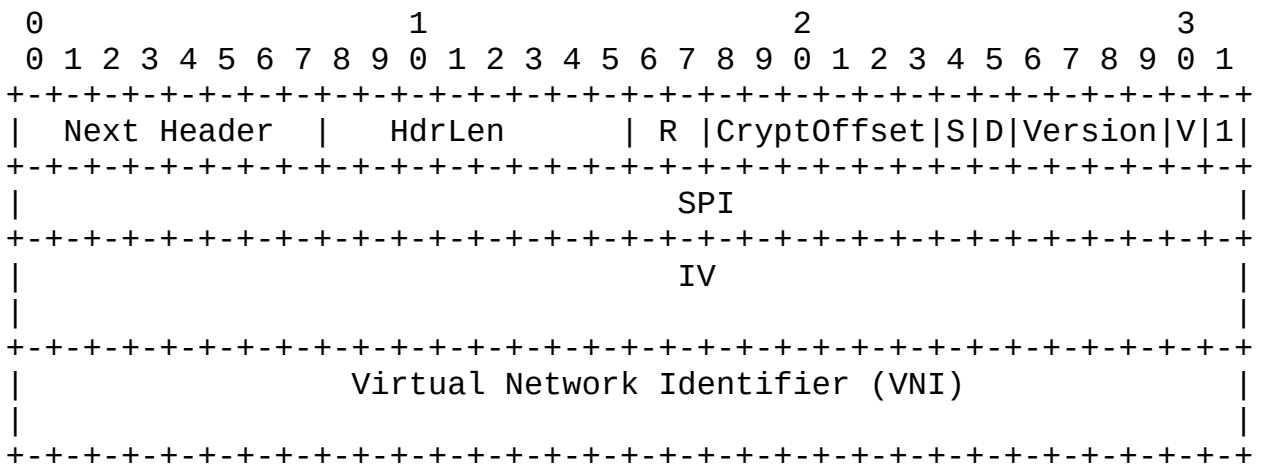

orig IP hdr (any options)
WESP Hdr
ESP Hdr
TCP
Data
ESP Trailer
ESP ICV
<--- (encryption) --->
<------- integrity ------->

Google PSP

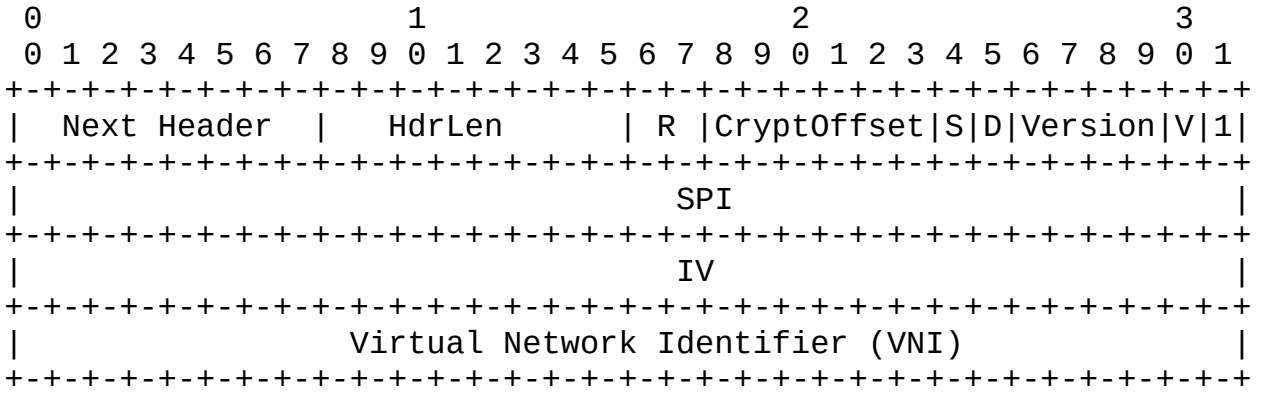
PSP

- Inspired by IPsec/ESP
- Hardware offload friendly
- Used for datacenter security
- Widely deployed at datacenters

PSP


0 1 2 3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
Next Header
HdrLen
R
CryptOffset
S
D
Version
V
1
SPI
IV
Virtual Network Identifier (VNI)
orig IP hdr (any options)
PSP Hdr
TCP
Pyld Data
PSP ICV
<- encryption ->
integrity

PSP



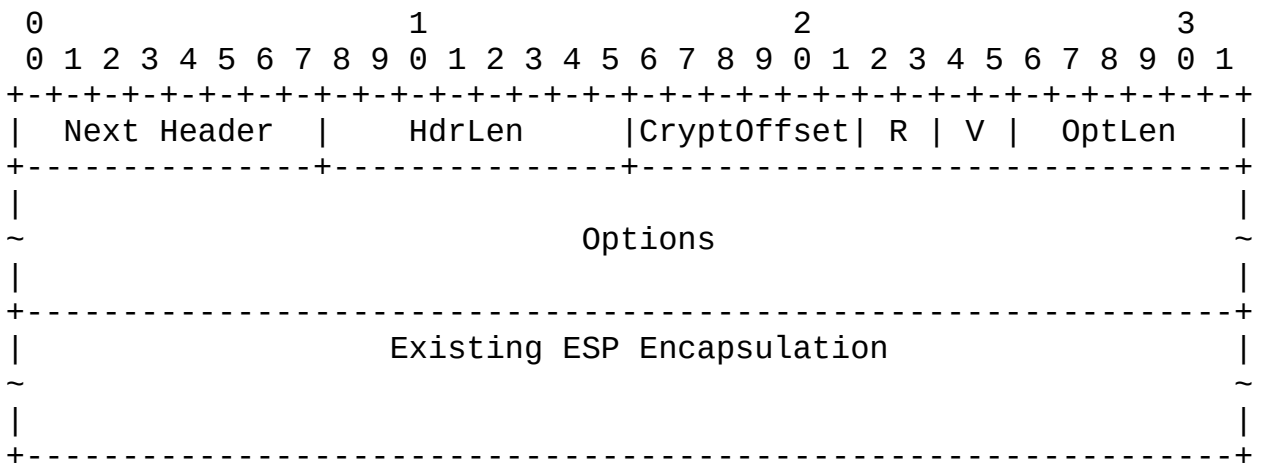
- CyptOffset – Can expose inner headers
- Version – Crypto parameters (algorithm type, keylen)
  - Stateless decryption on RX side
- VNI – Flow Identifier
- No sequence number
  - No replay protection

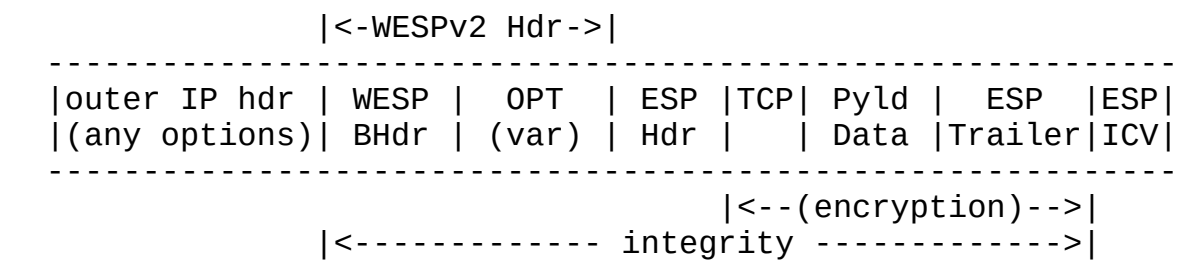
Wrapped ESP v2 (WESPv2)

WESPv2

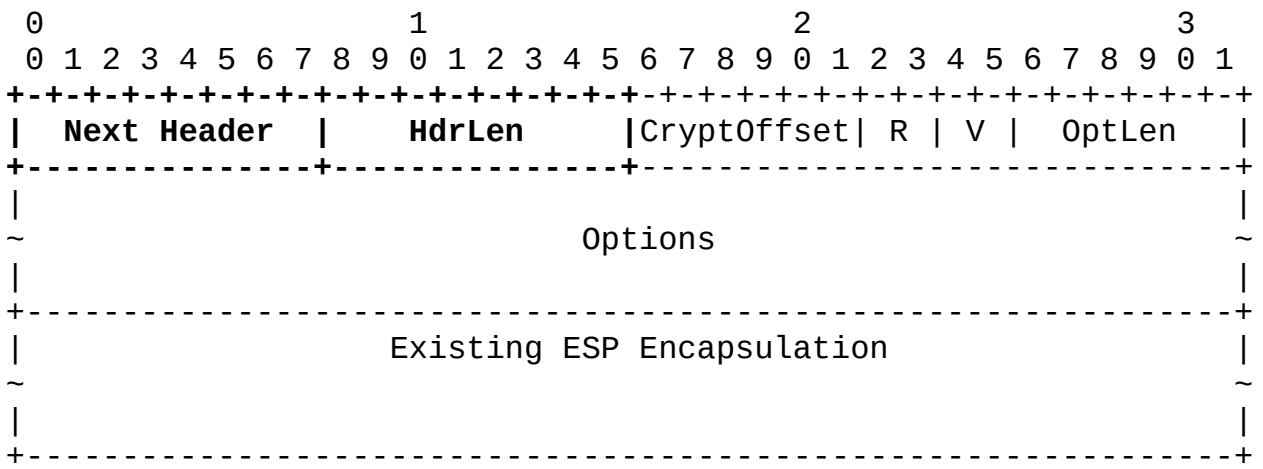
- WESP not widely used
- Has protocol number (141)
- Has version number
- Can match all PSP usecases
- Can carry integrity protected flow information
- Preserves original WESP usecase (partially)

WESPv2


0 1 2 3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
Next Header
HdrLen
CryptOffset
R
V
OptLen
Options
Existing ESP Encapsulation

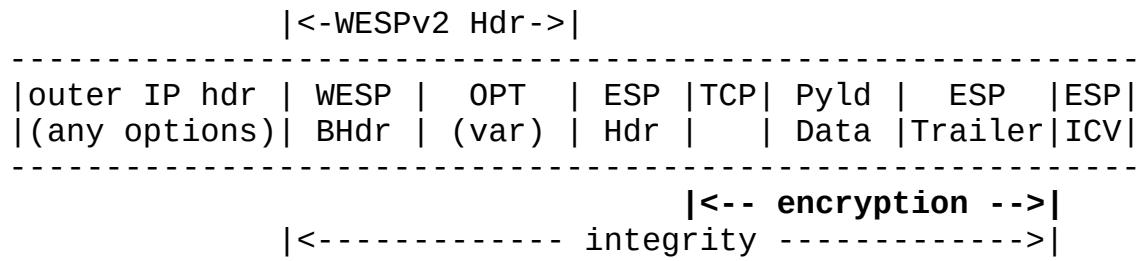

|<-WESPv2 Hdr->|
outer IP hdr (any options)
WESP BHdr
OPT (var)
ESP Hdr
TCP
Pyld Data
ESP Trailer
ESP ICV
|<--(encryption)-->|
|<------------ integrity ------------>|

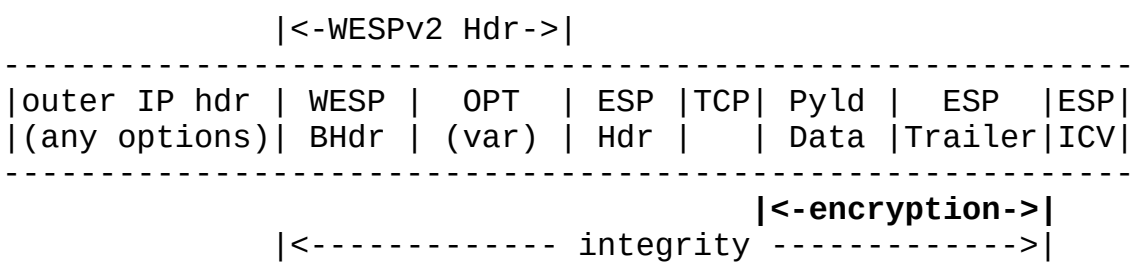
IPv6 Extension Header Style



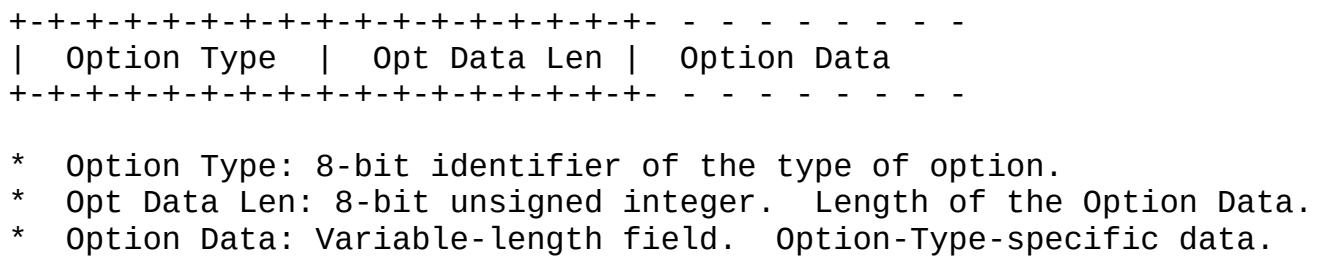
- Complient to RFC 8200 Section 4.8 (Defining new IPv6 Ext. Headers)

CryptOffset





WESPv2 Options



- Options are Type Length Values (TLV)
- Adapted from IPv6 Extension Header Options (RFC 8200 Section 4.2)
- Multiple Options can follow the header
- Future documents can define new Options
- Reserved space for private Options

Option Types

- Padding Options
- Flow Identifier Options
- Private Options
- Future documents can define new Option Types

Padding Options

- Used to align following header (4 byte IPv4, 8 byte IPv6)
- Future usecase: Ciphertext alignment (for SIMD, AVX)

Flow Identifier Options

- Must carry characteristic information of the inner flow
- Detailed specification of Flow Identifiers not in this draft
  - Must be provided by future documents
- Can be used by intermediate devices
  - ECMP
  - RSS

Private Options

- Reserved for private use
- Used for any purposes that are out of scope for standardization
- Can be used to encode hardware specific information

Usecases for Options

- Sequence number subspaces
  - draft-ponchon-ipsecme-anti-replay-subspaces-03
- VPN IDs
  - draft-he-ipsecme-vpn-shared-ipsecsa-00
- Padding for ciphertext alignment

Takeways from IPsec Workshop
and
Netdev Conference

Takeways

- WESPv2 design fits the PSP usecases
- PSP users are willing to migrate to a standardized packet format
- Cryptoffset is needed for telemetry
    - Mandatory for PSP usecase
    - Need to parse L4 headers
    - Never parses more then L4 header

Questions, suggestions?