IPsec Wrapped ESP (WESP) for Traffic Visibility

Sep 2009 Virtual IPsecme WG Meeting
22-Sep-2009

Ken Grewal

Gabriel Montenegro

Manav Bhatia

Current Status

- Advanced to IESG!
- Published rev08
  - included an applicability note suggested by the chairs to point out the existence and relationship with the heuristics document.
  - sundry nits.
- Publication Requested: Yaron's request for publication of rev08 as proposed standard RFC sent to AD (Pasi) on 03-Sep-2009
- More recently, Tero found that our flags field is not in consistent ordering with the rest of the packet.
- Fixed in rev09. Will submit once the AD comments are resolved.
- Status as of 22-Sep-2009: AD Evaluation:: Revised ID Needed:

  https://datatracker.ietf.org/idtracker/draft-ietf-ipsecme-traffic-visibility/

Open Items

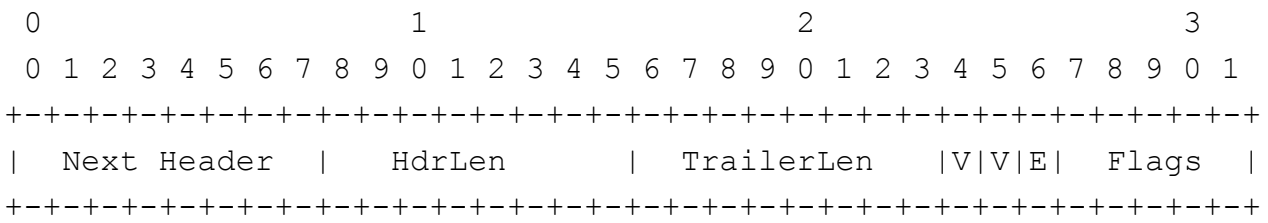
New ticket (#109) – WESP header alignment for IPv6
AD feedback from Pasi Eronen

- IPv6 requires extension headers to be aligned on 8-octet boundaries, and I believe this requirement applies to ESP, too (see e.g. RFC 4303 Section 2.3, 2nd paragraph). All current ESP specs (all encryption algorithms, UDP encapsulation, etc.) meet the 8-octet alignment requirement -- but adding a new four-octet header there obviously breaks it.
- Resolution:
  - We need an additional 4 bytes to ensure WESP header is on 8-byte alignment for IPv6
- Potential Solution:
  - Use one of the flag bits to signal the use of padding
  - Avoids padding for IPv4

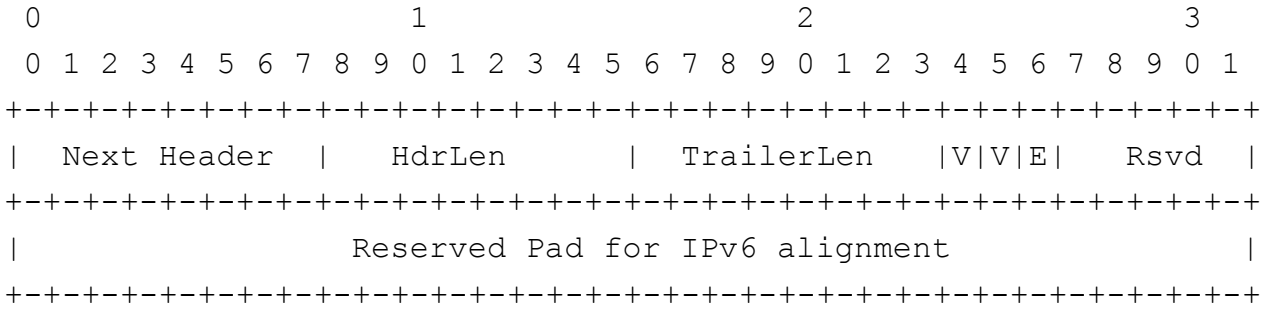
#109 – WESP header alignment for IPv6

Proposed Disposition

Existing WESP header definition



Proposed change

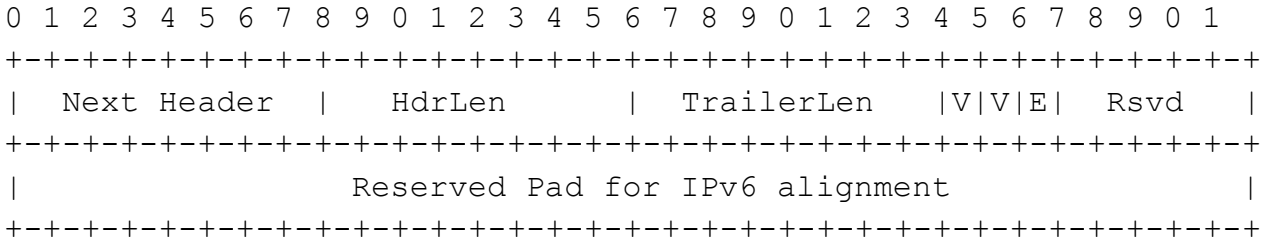


Note** This is not needed for IPv4

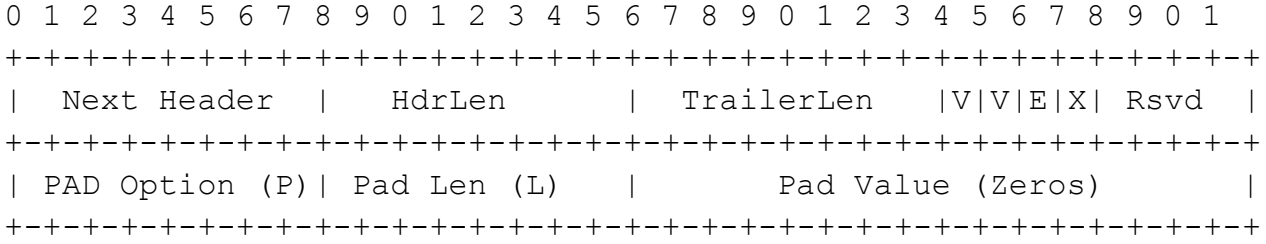
#109 – WESP header alignment for IPv6

Proposed Disposition

Proposed change for IPv6



Does it make sense to add semantics to this new field? Consider this…



WG Feedback?

Other Feedback

 # 104 Pasi: Integrity protection of the WESP header motivation

- **This item was discussed in the WG and closed**
  - http://trac.tools.ietf.org/wg/ipsecme/trac/ticket/104

Other (Minor) Comments:
Reopened #84 – Comments from Pasi below:

- The text currently uses "using ESP-NULL [RFC2410]" and "unencrypted" as synonyms. This was accurate before RFC4543, but is not any more. This needs some clarifying text somewhere (perhaps Section 1).
- Section 1 needs a sentence or two motivating the existence of the "E" bit -- currently it comes as a surprise to the reader later.

Resolution: Will craft text in rev 09

Other Feedback (#110)

Minor comments from Pasi:

Flags related

- Section 2/2.1: In Figures 1, 2, and 3, the bit numbers should be shifted one character to the right.
- Section 2: Change reserved flags notation from ‘Flags’ to ‘Rsvd’
- Flags bits notation LSB or MSB (will use MSB, as per rev09)

Resolution: Changes already in rev 09 to address a similar comment from Tero

HdrLen / TrailerLen related

- Add text HdrLen values less than 12 are invalid (and probably HdrLen values that are not multiple of 4 are invalid, and multiple of 8 for IPv6 case).
- TrailerLen scope only for ICV

Resolution: Changes in rev 09 as above

Other Feedback (#110)

Minor comments from Pasi (contd):

Misc related

- Section 2: "the packet must be dropped" -> "the packet MUST be dropped“
- Section 3: s/IPSec/IPsec/
- Section 4: this section is missing the allocation of SPI value 2 to indicate WESP from the "SPI Values" registry.
- Section 4 should say that for the WESP Version Number, the unassigned values are 1, 2, and 3.
- Section 6: [RFC4306], [RFC3948], and [RFC5226] should be normative references, not informative.

Resolution: Changes in rev 09 as above, but see below.

Discussion: ***IKEv2 (4306) is informative for ESP, so why would it be normative for WESP? Similarly for UDP Encap via 3948***

Other Feedback (#110)

Minor comments from Pasi:

Misc related

- The figures in 2.2.1 and 2.2.2 are very confusing, since they suggest WESP could be applied as a separate step after ESP processing…
- Option 1: Keep these figures (check ‘before’ figures to raw packet)
- Option 2: Remove these figures altogether

Resolution: Keep figures or remove?