Minimal ESP

Migault - Guggemos

Motivation

Kernel implementation of ESP fits multiple purpose usage of these OS with most options.

- Performed at the expense of resources, or a lack of performance.
- Constrained devices are likely to have an optimized ESP implementation adapted to their specificities.

With the adoption of IPsec by IoT devices with minimal IKEv2, ESP Header Compression (EHC) it becomes crucial that ESP implementation designed for constrained devices remain inter-operable with the standard ESP implementation to avoid a fragmented usage of ESP.

Scope

This document describes the minimum set of properties an ESP implementation needs to meet.

The document provides guidance on implementation experience:

- Remain fully compatible to IPsec/ESP
- Recommendation on how to build all IPsec/ESP fields
- Recommendation on crypto-suites to implement

IPsec / ESP

```
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
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+ ----
|               Security Parameters Index (SPI)                 | ^Int.
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+ |Cov-
|                      Sequence Number                          | |ered
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+ | ----
|                    Payload Data* (variable)                   | |   ^
~                                                               ~ |   |
|                                                               | |Conf.
+               +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+ |Cov-
|               |     Padding (0-255 bytes)                     | |ered*
+-+-+-+-+-+-+-+-+               +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+ |   |
|                               |  Pad Length   | Next Header   | v   v
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+ ------
|         Integrity Check Value-ICV   (variable)                |
~                                                               ~
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

ESP Parameters

Security Parameters Index (SPI) [Mandatory 32 bits]:

- For single connection device: predefined SPIs / IPv4 / MAC / IPv6

Sequence Number (SN) [Mandatory 32 bits]:

- To avoid maintaining a counter: time may be used

ESP Parameters

Padding [variable] / Pad Length [Mandatory 8 bits]:

- Address the 32 bit IPv4 Header and 64 bit IPv6 Header alignment
- May be part of the encryption (AES-CBC 128 bit block size)
- May not be part of IPsec/ESP:
  - Set Padding to Zero instead of random, counters…
  - Document impact of fixed size data on Padding

Next Header (NH) [Mandatory 8 bits]:

Updates

The document has been reviewed and will continuously reviewed by IPsecme WG

- Already in good shape to reach the LWIG Milestone

This is aligned with efforts to adapt IPsec for constrained devices:

- IPsecme
- LWIG (minimal IKEv2)

We have internal implementation (C)

We would like the document being adopted as WG document

Thanks you!