Minimal ESP

draft-mglt-lwig-minimal-esp-05

Migault, Guggemos -- IETF99

Motivations

Securing m2m communications with IPsec/ESP presents significant advantages [1] especially for small devices:

- Interoperability
- VPN
- Transport layer independent
- Key management independent
- Lower overhead
- ...

[1] https://www.ietf.org/proceedings/96/slides/slides-96-6lo-9.pdf

Motivations

IPsec/ESP [RFC4303] is likely to be implemented / deployed by constrained devices, this document describes and provides recommendations to implement a minimal IPsec/ESP that remains interoperable with the standard IPsec/ESP [RFC4303]:

- Mandatory features
- Implementation optimization for constrained devices

This document is expected to companion the Minimal IKEv2 Initiator Implementation [RFC7815]

History

Minimal ESP has been presented in LWIG during IETF96 [1].

- The document needed more reviews.

Minimal ESP has been reviewed in IPSECME during IETF98 [2].

- We believe the new version is ready for adoption

[1] https://www.ietf.org/proceedings/96/slides/slides-96-lwig-3.pdf
[2] https://www.ietf.org/proceedings/98/slides/slides-98-ipsecme-minimal-esp-00.pdf

Change since 04

- Clarifying the purpose of a minimal implementation (Tero, Scott)
  - Clarifying text in the abstract / introduction
- SPI: (Scott, Daniel)
  - We included some recommendation on how to index the SA with the SPI.
  - We also presented different lookups for anycast and multicast nodes.
  - We detailed how to avoid generating random SPI, and instead use fix SPI.
  - We clarify the text to avoid it being interpreted as there is no need for random generators.
- Padding: (Scott, Yoav and Tero)
  - Padding was corrected and mentioned as mandatory
  - TFC has been mentioned as not being implemented in a minimal version.

Change since 04

- Next Header: (Scott, Tero)
    - The Next Header section has been updated by specifying better position the minimal implementation regarding the dummy packet as well as the BEET mode.
    - The ability to reject dummy packet has been added as being mandatory for a minimal implementation.
- ICV (Valery, other people in the WG)
    - Text was clarified to avoid the text being interpreted as making ICV optional.

Next step

We want to continue having Minimal ESP discussions in LWIG as well as IPSECME.

We believe the draft has been sufficiently discussed for adoption in LWIG.

4 known implementations:

- user land library (in C, python),
- support for Contiki, RIOT (to be released)

Thanks!