Minimal ESP

Migault, Guggemos
draft-mglt-lwig-minimal-esp-04.txt

Scope

This document describes a minimal version of the IP Encapsulation Security Payload (ESP) described in RFC 4303 which is part of the IPsec suite.

This document does not update or modify RFC 4303, but provides a compact description of how to implement the minimal version of the protocol.

SPI

General case:

- RECOMMENDED to randomly generate the SPI

Some constraint nodes cannot generate a random SPI:

- When a constraint node uses a fix value as a SPI, it is RECOMMENDED the constraint node has as many SPI values as ESP session per host, and that lookup includes the IP addresses.
    - Problem when a gateway does not implements a longest match prefix.

Fix SPI comes with privacy issues

SN, Padding, NH

SN:

- Mandatory, but can be implemented with counter or clock

Padding:

- Can be done by the encryption algorithm (AES CBC) or ESP (AES GCM/CCM)

NH:

- Mandatory, but can be implemented with a fix value.

ICV, Crypto suites

ICV:

- Optional, but recommended to use authenticated encryption

Cryptographic suites:

- Implementer SHOULD follow the recommendations provided by [I-D.ietf-ipsecme-rfc7321bis] and updates.

Thanks!