Modes of Operation for SEED for Use with IPSec

Seokung Yoon (KISA)

Overview

- The RFC4196 only specifies the use of the SEED cipher in the CBC mode within Encapsulation Security Payload (ESP)

- draft-seokung-ipsecme-seed-ipsec-modes-00 updates RFC4196, to include the use of the SEED block cipher algorithm in operation modes as an IPsec ESP mechanism

  - Counter Mode (CTR), Counter with CBC-MAC (CCM) Mode and Galois/ Counter Mode (GCM)

  - SEED in CTR, CCM and GCM modes is used in IPSec as AES. The only difference in the processing is that SEED-XXX uses SEED as the underlying encryption primitive

IKEv2 Conventions

- describes the conventions used to generate keying material and nonces / salt values for use with CTR/CCM/GCM using IKEv2

  - SEED-CTR key is 20 octets. The first 16 octets are the 128-bit SEED key, and the remaining four octets are used as the nonce value

  - SEED-CCM key is 19 octets. The first 16 octets are the 128-bit SEED key, and the remaining three octets are used as the salt value

  - SEED-GCM key is 20 octets. The first 16 octets are the 128-bit SEED key, and the remaining four octets are used

Future Work

- Add test vectors for operation modes
- Modify some editorial nits