Implicit IV for AES-CBC, AES-CTR, AES-CCM and AES-GCM

draft-mglt-6lo-aes-implicit-iv-01.txt

D. Migault, T. Guggemos

27/03/2015- IETF92- Dallas

Motivation

In the context of IoT:

- Sending extra bytes » Computation

To make devices last longer:

- We are looking at reducing the networking overhead

Currently IV is sent in every packet

- We define how IV can be generated instead of being sent.

The work is jointly done with 6lo / 6lo-security groups

IV compression

IVs have different properties the draft considers two categories:

- AES CBC (16 byte IV, random and unpredictable)
- AES-CTR, AES-CCM and AES-GCM (8 byte IV MUST NOT repeat)

The main idea is to:

- Generate an IV that respects IV properties
- Bind each ESP packet with a IV value

Questions

A few questions have been raised for this draft:

- Enough entropy for AES-CBC
- Certification processus may require the IV to be in the packet

Thank you for your attention