           Implicit IV for AES-CBC, AES-CTR, AES-CCM and AES-GCM
                  draft-mglt-6lo-aes-implicit-iv-01.txt

Abstract

   IPsec ESP with AES-CBC, AES-CTR, AES-CCM or AES-GCM sends an IV in
   each IP packet, which represents 8 or 16 additional bytes.

   In some context, such as IoT, the cost of sending bytes over
   computing these bytes is generally in favor of the computation. As a
   result, it would be better to compute the IV on each party then to
   send it.

   The document describes how to the IV can be generated instead of
   being sent. This document limits the IV generation for AES-CBC, AES-
   CTR, AES-CCM and AES-GCM but can be used for additional cryptographic
   mode and suites.

Status of This Memo

   This Internet-Draft is submitted in full conformance with the
   provisions of BCP 78 and BCP 79.

   Internet-Drafts are working documents of the Internet Engineering
   Task Force (IETF). Note that other groups may also distribute
   working documents as Internet-Drafts. The list of current Internet-
   Drafts is at http://datatracker.ietf.org/drafts/current/.

   Internet-Drafts are draft documents valid for a maximum of six months
   and may be updated, replaced, or obsoleted by other documents at any
   time. It is inappropriate to use Internet-Drafts as reference
   material or to cite them other than as "work in progress."

   This Internet-Draft will expire on August 21, 2015.

Copyright Notice

Table of Contents

1. Requirements notation

   The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT",
   "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this
   document are to be interpreted as described in[RFC2119].

2. Introduction

   Using AES in one of the AES-CBC [RFC3602], AES-CTR [RFC3686]
   encryption mode, or in one of the AES-CCM [RFC4309] and AES-GCM
   [RFC4104] combined requires the specification of an IV for each ESP
   packet. Currently this IV is sent in each ESP packet [RFC4303].

   IoT devices present new characteristics over traditional devices.
   One of them is that the balance between extra computation and extra
   byte sent over the wire is most of the time in favor of extra
   computation. For such devices, embedding the IV in each packet
   constitutes an extra cost over computing the IV of each associated
   packet.

   Depending on the the AES mode, the IV can be of different sizes and
   have different properties. AES-CBC needs a 16 byte IV. This IV MUST
   be chosen at random and MUST be unpredictable. In addition IV MUST
   NOT be generated with low Hamming distance (like counter) for example
   -- [RFC3602] Section 3. AES-CTR and AES-CCM need an 8 byte IV. This

IV MUST be unique ([RFC3686] Section 2.1). Finally, AES-GCM requires
8 byte IV, that must be unique for a given key -- [RFC4104]
Section 2.

This document defines how for each of the AES-CBC, AES-CTR, AES-CCM
and AES-GCM, the IV can be computed by each peer instead of being
included in the ESP packet.

This document limits its scope to AES as most of devices in the IoT
have hardware acceleration for AES, and use AES. However, the
description may be extended to additional crypto suites.

3. Terminology

   - IoT: Internet of Things

   - IV: Initialization Vector

4. Implicit IV with AES CBC

   With AES-CBC, the IV is 16 bytes, random and unpredictable. In this
   document, the binding between IV and ESP packet is performed using
   the Sequence Number or the Extended Sequence Number. A clear text
   payload is derived from the Sequence Number or the Extended Sequence
   Number. In order to generate the IV randomly, AES is used as a
   random permutation. A dedicated 16 byte key is used for each peer.
   key_iv_initiator (resp. key_iv_responder) is used to derive the IV
   emitted by the initiator (resp. the responder).

   Keys key_iv_initiator and key_iv_responder MUST be agreed prior IPsec
   packets are exchanged. When IKEv2 [RFC7296] is used these keys are
   derived from the KEYMAT. key_iv_initiator is the first key generated,
   followed by key_iv_responder.

   Figure 1 (resp. Figure 2) defines a clear text payload derived from
   a 4 byte Sequence Number (resp. a 8 byte Extended Sequence Number)

```
 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
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
|                             Zero                              |
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                        Sequence Number                        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```
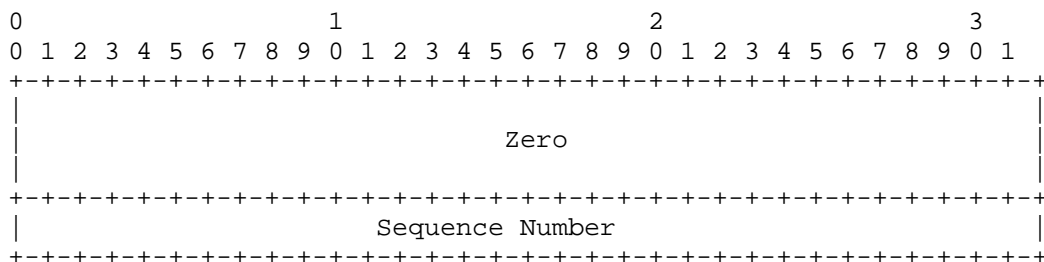
                Figure 1: Clear Text Payload for AES-CBC

   Where,

   - Sequence Number: the 4 byte Sequence Number carried in the ESP
      packet.

   - Zero: a 12 byte array with all bits set to zero.

```
 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
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                             Zero                              |
|                                                              |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                           Extended                           |
|                      Sequence Number                         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```
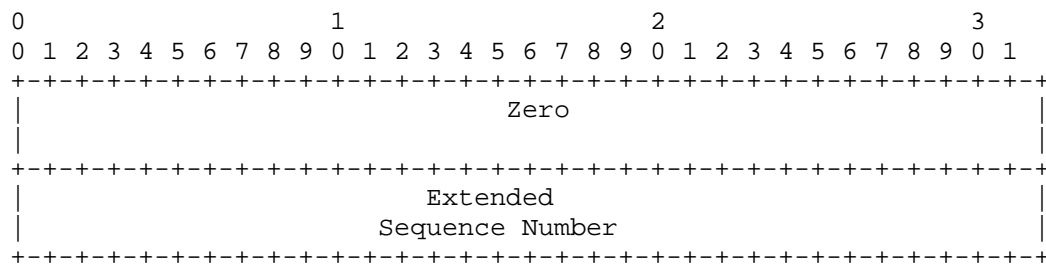
         Figure 2: Clear Text Payload for AES-CBC with Extended Sequence
                                   Number

   Where,

   - Extended Sequence Number: the 8 byte Extended Sequence Number of
      the Security Association. The 4 byte low order bytes are carried
      in the ESP packet.

   - Zero: a 8 byte array with all bits set to zero.

5. Implicit IV with AES-CTR, AES-CCM and AES-GCM

   With AES-CTR, AES-CCM and AES-GCM, the 8 byte IV MUST NOT repeat.
   The binding between a ESP packet and its IV is provided using the
   Sequence Number or the Extended Sequence Number. Figure 3 (resp
   Figure 4) represents the IV with a regular 4 byte Sequence Number
   (resp. a 8 byte Extended Sequence Number).

```
 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
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                             Zero                              |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                        Sequence Number                       |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

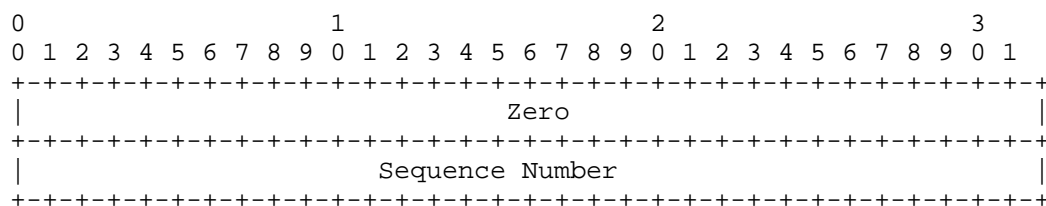   Figure 3: IV for AES-CTR, AES-CCM and AES-GCM with 4 byte Sequence
                                   Number

   Where,

- Sequence Number: the 4 byte Sequence Number carried in the ESP
  packet.

- Zero: a 4 byte array with all bits set to zero.

```
 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
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                         Extended                              |
|                     Sequence Number                           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

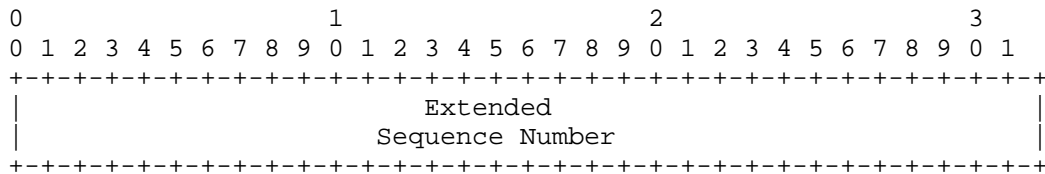   Figure 4: IV for AES-CTR, AES-CCM and AES-GCM with 8 byte Extended
                             Sequence Number

Where,

- Extended Sequence Number: the 8 byte Extended Sequence Number of
  the Security Association. The 4 byte low order bytes are carried
  in the ESP packet.

6. Security Consideration

   IV generation of the AES-CBC, AES-CTR, AES-CCM and AES-GCM have not
   been explicitly defined. It has been left to the implementation as
   long as certain security requirements are met. This document
   provides an explicit and normative way to generate IVs. The
   mechanism described in this document meets the IV security
   requirements of AES-CBC, AES-CTR, AES-CCM and AES-GCM.

   Randomness is provided by using AES. If this hypothesis is no longer
   valid, than most probably, none of the AES mode will be considered
   secure.

7. IANA Considerations

   Each of the AES-CBC, AES-CTR, AES-CCM and AES-GCM crypto suite needs
   to have their associated cryptographic suite with implicit IV. That
   is to say the transforms below should be added to the Transform Type
   1 - Encryption Algorithm Transform IDs:

- ENCR_AES_CBC_IMPLICIT_IV

- ENCR_AES_CTR_IMPLICIT_IV

- ENCR_AES-CCM_8_IMPLICIT_IV

- ENCR_AES-CCM_12_IMPLICIT_IV

   - ENCR_AES-CCM_16_IMPLICIT_IV

   - AES-GCM with 8 octet ICV and implicit IV

   - AES-GCM with 12 octet ICV and implicit IV

   - AES-GCM with 16 octet ICV and implicit IV

8. Normative References

   [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate
              Requirement Levels", BCP 14, RFC 2119, March 1997.

   [RFC3602] Frankel, S., Glenn, R., and S. Kelly, "The AES-CBC Cipher
              Algorithm and Its Use with IPsec", RFC 3602, September
              2003.

   [RFC3686] Housley, R., "Using Advanced Encryption Standard (AES)
              Counter Mode With IPsec Encapsulating Security Payload
              (ESP)", RFC 3686, January 2004.

   [RFC4104] Pana, M., Reyes, A., Barba, A., Moron, D., and M. Brunner,
              "Policy Core Extension Lightweight Directory Access
              Protocol Schema (PCELS)", RFC 4104, June 2005.

   [RFC4303] Kent, S., "IP Encapsulating Security Payload (ESP)", RFC
              4303, December 2005.

   [RFC4309] Housley, R., "Using Advanced Encryption Standard (AES) CCM
              Mode with IPsec Encapsulating Security Payload (ESP)", RFC
              4309, December 2005.

   [RFC7296] Kaufman, C., Hoffman, P., Nir, Y., Eronen, P., and T.
              Kivinen, "Internet Key Exchange Protocol Version 2
              (IKEv2)", STD 79, RFC 7296, October 2014.

Appendix A. Document Change Log

   [draft-mglt-ipsecme-diet-esp-IV-generation-00.txt]: changing
   affiliation.

   [draft-mglt-ipsecme-diet-esp-IV-generation-00.txt]: First version
   published.

Authors' Addresses

    Daniel Migault (editor)
    Ericsson
    8400 boulevard Decarie
    Montreal, QC H4P 2N2
    Canada

    Email: mglt.ietf@gmail.com

    Tobias Guggemos (editor)
    LMU Munich
    Am Osteroesch 9
    87637 Seeg, Bavaria
    Germany

    Email: tobias.guggemos@gmail.com