Implicit IV for Counter-based Ciphers in IPsec

DRAFT-MGLT-IPSECMH-IMPLICIT-IV
YOAV NIR, DANIEL MIGAULT, TOBIAS GUGGEMOS – IETF 99 – PRAGUE
Update from version 02

Address the main comment from Eric:

This document does not consider AES-CBC ([RFC3602]) as AES-CBC requires the IV to be unpredictable. Deriving it directly from the packet counter as described below is insecure as mentioned in Security Consideration of [RFC3602] and has led to real world chosen plain-text attack such as BEAST [BEAST].

We will publish the ietf draft and think we are ready for WGLC.
Thanks!
Why?

- Counter-based algorithms and AEADs are becoming more popular: AES-GCM, AES-CCM, ChaCha20.

- Unlike CBC-based algorithms, these do not benefit from unpredictable IVs. In fact, the specifications for all of these recommend using a guaranteed unique IV, specifically a counter as the recommended method of setting this IV.
ESP Header

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
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|               Security Parameters Index (SPI)               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                          Sequence Number                     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                  IV        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
This is a packet sequence number
**ESP Header**

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
</tbody>
</table>
| +---------------------+---------------------+---------------------+---------------------+
| | Security Parameters Index (SPI) | | +---------------------+---------------------+---------------------+---------------------+
| | Sequence Number | | +---------------------+---------------------+---------------------+---------------------+
| | IV | | +---------------------+---------------------+---------------------+---------------------+
| | | | +---------------------+---------------------+---------------------+---------------------+
| | | | | +---------------------+---------------------+---------------------+---------------------+

So is this
Implicit IV

- If we follow the recommendations, those two counters will be equal.
- So why do we need to repeat the same counter in two different fields?
- We don’t.
- If both sides agree, we can just omit the IV.
- It’s optional anyway.
- Saves 8 bytes per packet.
Negotiating Implicit IV

- New Transform ID
  - ENCR_AES-CCM_8_IIV
  - ENCR_AES-GCM_16_IIV
  - ENCR_CHACHA20-POLY1305_IIV