Implicit IV for Counter-based Ciphers in IPsec

DRAFT-MGLT-IPSECMEM-IMPLICIT-IV

YOAV NIR – IETF 96 - BERLIN
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

<table>
<thead>
<tr>
<th>Security Parameters Index (SPI)</th>
</tr>
</thead>
<tbody>
<tr>
<td>---------------------------------</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Sequence Number</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>IV</th>
</tr>
</thead>
</table>

<p>| |</p>
<table>
<thead>
<tr>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>
This is a packet sequence number
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

Options:
- New Transform Type
  - ENCR, INTEG, PFS, ESN, and now: IIV
- New Transform Attribute
  - Key Length. Now also IIV
- New Transform ID
  - Already have AES-GCM_16; now also AES-GCM_16_IIV
- New Notification
Please Adopt Me