IKEv2 Count Based SA Extension

Migault, Liu, Zhang
Problem Statement

Hardware accelerated IPsec:

- Are designed for a fix number of SAs
- SAs that cannot be created result in traffic being rejected.

Simultaneous IKEv2 rekeys result in the creation of redundant SAs

- underutilisation of the hardware component
SAs lifetime can be expressed using a time or a byte count limit.

Time limit:

- makes limit predictable (over time)
  - it is easy to anticipate the expiration time
- Uniformly randomizing time limit distributes the IKEv2 rekey uniformly
  - and works pretty well

Byte count limit:

- are hard to predict - as it depends on the traffic.
  - our implementation checks every 2s which SAs needs to be rekeys
- the randomization does not compensate the traffic bursts
As a result, count bases SA results in multiple redundant rekey.

Why we want to use byte count limit?
- A direct expression of the lifetime of the cryptographic key.
- Binding the SA life time to traffic is appropriated for device that can be in long sleeping mode.

The document describes an IKEv2 extension that prevents redundant rekey:
- No magic: peers agree who is expected to start the rekey.
Initiator                         Responder
-------------------------------------------
HDR, SAi1, KEi, Ni  -->
      HDR, SAi2, KEr, Nr, [CERTREQ]
HDR, SK {IDi, [CERT,] [CERTREQ,]
      [IDr,] AUTH, SAi2,
    TSi, TSr, N(COUNT_BASED_SA_PROPOSED)}  -->
      HDR, SK {IDr, [CERT,] AUTH,
    SAi2, TSi, TSr, N(COUNT_BASED_SA_SELECTED)}
COUNT_BASED_SA_PROPOSED Notification Data contains for each Transform ID:

- Acceptable count base life time
- Rekey Value (random)
COUNT_BASED_SA_SELECTED Notification Data

<table>
<thead>
<tr>
<th>1</th>
<th>2</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>+------------------------------------------------------------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Rekey Value</td>
<td></td>
</tr>
<tr>
<td>+------------------------------------------------------------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Count Based SA Life Time Value (LT)</td>
<td></td>
</tr>
<tr>
<td>+------------------------------------------------------------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>+------------------------------------------------------------------</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
1. Selection of the initiator for the next rekey:
   - The peer with the greatest Rekey Value is designated to initiate the next rekey.
   - In case of equality, the current initiator remains the initiator.

2. Setting the Hard (H) and Soft (S) count base SA lifetime:

   - Initiator:
     - $S = X_i \times LT + \text{rand}(0, 5\% \times LT)$ with $X_i \leq 80\%$
     - $H = LT$

   - Responder:
     - $S = X_r \times LT + \text{rand}(0, 5\% \times LT)$ with $X_r \geq 95\%$
     - $H = LT$
Thanks!