GDOI Update Draft

Sheela Rowles
IETF 73 Minneapolis
November 19, 2008
GDOI delete capability

• RFC 3547 specifies that keys can be deleted by sending an ISAKMP Delete payload as part of a GDOI GROUPKEY-PUSH message specifying the spi of the key to be deleted.

• There may be circumstances where the GCKS wants to start over with a clean slate.
Add flexibility to delete all the policy

- No longer confident about the integrity of the group: send SPI = 0 in DELETE payload.

<table>
<thead>
<tr>
<th>Action</th>
<th>DOI</th>
<th>SPI</th>
<th>Protocol_id</th>
</tr>
</thead>
<tbody>
<tr>
<td>Delete TEK with ‘valid TEK SPI’</td>
<td>GDOI</td>
<td>valid TEK SPI</td>
<td>TEK</td>
</tr>
<tr>
<td>Delete KEK with ‘valid KEK SPI’</td>
<td>GDOI</td>
<td>Valid KEK SPI</td>
<td>0</td>
</tr>
<tr>
<td>Delete All TEK(s)</td>
<td>GDOI</td>
<td>0</td>
<td>TEK</td>
</tr>
<tr>
<td>Delete All KEK(s)</td>
<td>GDOI</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
Remove PFS

- AES keys are much more common
- Need for PFS is an overstated threat for IKE phase 1 keys.
  - Need to take out verbage in update draft
  - Need to clarify in update draft that section 3.2.1 (PFS) of RFC3547 is not needed.
  - Can deprecate the KEK attribute KE_OAKLEY_GROUP
Other changes

• Due to draft-ietf-msec-ipsec-extensions-09.txt
• TEK attribute
• KEK attributes
New IPsec SA Attribute

• The GDOI update draft needs to be updated to reflect the new SA attribute representing directionality in an SPD entry.
  – Swap address & ports from section 4.1.1 of multicast extensions draft.
  – Following will be specified:
    • Default behavior will be to swap and require that the attribute is sent for ‘no swap’.
New Group Attributes

• A couple of new group attributes need to be specified based on the extensions draft to improve interoperability. (section 4.2.1)
  – ATD: Activation Time Delay
    • specific amount of time GDOI holds onto the key before installing to ipsec.
  – DTD: Deactivation Time Delay
    • specific amount of time before deactivating a key.
Updates will be in next version of draft


• Currently sitting in the editor’s queue