Least-Common Scope Communications

Dusan Mudric, Ciena
Alexandre Petrescu, CEA LIST
Problem Statement

- **Hb-Hd**: GUA for signaling and media sockets on SITE-2
- Sockets listening on global addresses are exposed to attacks
Problem Statement - cont

- RFC6724: DASA Rule 8 prefers a destination address with the smallest scope.
- Applications don't always have LL candidate address.
- An application will open a socket using GUA, even for GUA on a local link => exposed to attacks via globally reachable socket address.
Proposed Solution (LL Address Resolution)

- To avoid these attacks use Link Local addresses for on-link communications
- Find a destination Link-Local address that is assigned to the same interface as an on-link GUA
**Neighbor Solicitation 'L' bit**

- For LL address resolution, 'L' flag is added to NS message
- NS Target-Address: is on-link GUA
- NS Source Address: if L bit is set, LL address
- NS Destination Address: GUA or Solicited Node Multicast Address
- NA: The target returns its LL address in the Target Link-Local Address Option
NS 'L' Bit Definition

IP Fields:

Source Address
If L bit is set, either LL address assigned to the interface from which this message is sent or (if Duplicate Address Detection is in progress [ADDRCONF rfc4861]) the unspecified address.

Destination Address
Either the solicited-node multicast address corresponding to the target GUA or ULA address, or the target GUA or ULA address.

ICMP Fields:
L
Link Local flag. When set, the L-bit indicates that the sender is requesting Link Local address from the target.

Figure 1: NS with 'L' bit
NA Target Link-Local Address Option

<table>
<thead>
<tr>
<th>0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
</tr>
<tr>
<td>---------------------------------------------</td>
</tr>
<tr>
<td>R</td>
</tr>
<tr>
<td>---------------------------------------------</td>
</tr>
<tr>
<td>+</td>
</tr>
<tr>
<td>Target Address</td>
</tr>
<tr>
<td>+</td>
</tr>
<tr>
<td>Options ...</td>
</tr>
<tr>
<td>+</td>
</tr>
</tbody>
</table>

IP Fields:

Source Address
- If NS L bit is set, LL address of the same GUA target interface is provided

Possible options:

Target Link-Local address
- The Link Local address of the same GUA target, the sender of NA.
  This option MUST be included if NS L bit is set and LL is available.

  Type: 4 (Target Link Local address)
  Length: 16 bytes
  Link Local Address: e.g. fe80:0:0:0:aa:bb:cc:dd

Receivers MUST silently ignore this option if they do not recognize it and continue processing the message.

Figure 2: NA for LL address resolution
Questions?

- Thank you