Geneve Security Requirements

Migault, Boutros, Wings, Krishnan
Goals

Geneve security without transit devices

Geneve security with transit devices

- Problem
- Moving forward
Geneve NVE-to-NVE

In a NVE-to-NVE communication without transit devices:

- Options a, b, c are treated by the NVE
- DTLS or IPsec are very well known protocol to secure this communication
Geneve NVE-to-NVE

- NVE
  - Option a, b, c
  - Payload
    - Options a, b, c, d
    - Geneve (Fixed Header)
      - UDP
      - IP

- NVE
  - Option a
  - Payload
    - Options a, b, c, d
    - Geneve (Fixed Header)
      - UDP
      - IP
Geneve NVE-to-NVE
Geneve with Transit Devices

Options a, b, c are treated by the NVE (a) and the Transit Device (b, c)

The problem of DTLS is that it is either:

- activated: Transit device does not see it
- not activated: no protection
Geneve with Transit Devices

- NVE
  - Option a, b, c

- Payload
  - Options a, b, c, d
  - Geneve (Fixed Header)
  - UDP
  - IP

- Transit Device
  - Option b, c
  - Payload
  - Options a, b, c, d
  - Geneve (Fixed Header)
  - UDP
  - IP

- NVE
  - Option a
  - Payload
  - Options a, b, c, d
  - Geneve (Fixed Header)
  - UDP
  - IP
## Geneve with Transit Devices

<table>
<thead>
<tr>
<th>NVE</th>
<th>Transit Device</th>
<th>NVE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option a, b, c</td>
<td>Option b, c, d</td>
<td>Option a</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Payload</th>
<th>Options a, b, c, d</th>
<th>Geneve (Fixed Header)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Options a, b, c, d</td>
<td>Geneve (Fixed Header)</td>
<td>Geneve (Fixed Header)</td>
</tr>
<tr>
<td></td>
<td>IP</td>
<td>UDP</td>
</tr>
<tr>
<td></td>
<td>DTLS</td>
<td>DTLS</td>
</tr>
<tr>
<td></td>
<td>UDP</td>
<td>UDP</td>
</tr>
<tr>
<td></td>
<td>IP</td>
<td>IP</td>
</tr>
</tbody>
</table>
Transit Devices

The current Geneve specification mentions TD can ONLY READ Geneve Options.

- We need to enforce that actions are limited to READ and detect write
  - authentication
- We need to be able to limit the options a TD can read
  - encryption
Geneve with Transit Devices
Transit Devices

Transit Devices are not defined in the NVO3 architecture (RFC8014):

- more work is needed to specify their place in the architecture.
- there is a need to clarify the boundaries between TD and NVE

Typically, what happens when multiple transit devices are on path?

- should an option visible to a TD be visible to all TD?
- should options visible to a TD be only visible to that TD?
- could an option for a TD be encrypted, authenticated?
Next Steps

Define Transit Devices

Define Security Requirements

Define Security Architecture, Encrypted / Authenticated options