Draft Geneve update

IETF 102 Montreal, NVO3 WG meeting

Ilango Ganga, T. Sridhar

Jul 18, 2018

Draft Geneve -07 update

- Draft Geneve was updated on Jul 02nd with the following changes
  - draft-ietf-nvo3-geneve-07

  - Clarification on the role of transit devices
  - Updated Security Considerations section per BCP 72 guidelines
  - Updated option class assignment table

Clarification on the role of transit devices

- Per Geneve architecture, transit devices do not originate or terminate the geneve packet, that is the responsibility of end points
    - There were some queries (or mis-interpretation) on the role of transit devices during security requirements and IOAM discussions, hence we added clarifying statements to make it clear on what the transit devices can and cannot do
    - As non-terminating devices, transit devices MUST NOT insert or delete options as that is the responsibility of endpoints
        - Transit devices MAY be able to interpret the options, but this is OPTIONAL
        - Options or their ordering MUST NOT be changed by transit devices
    - Also note that, transit devices MUST not attempt to interpret or process Geneve OAM packets – no changes to the draft, just reiterating the original text

Security Considerations section

- We received feedback from recently completed RFC (RFC8300) review process that Security Considerations section should be updated per BCP 72 guidelines
- Hence we updated the section to highlight potential security risks that may be applicable to Geneve deployments and approaches to mitigate such risks. We have included subsections on the following
  - Data confidentiality
  - Data integrity
  - Authentication of NVE peers
  - Multicast/Broadcast, and Control plane communications handling

Security Considerations section (Contd.)

- Not all risks outlined are applicable to all deployments, for example, there could be risks that may only be applicable to public cloud/multi-tenant deployments and those risks may not be applicable to private data center deployments
- So a data center operator should do risk assessment applicable to their infrastructure and mitigate those risks accordingly
- We have included sufficient description in subsections to outline the scenarios where such requirements are applicable
- There was a comment (on draft 07) that certain requirements may not be applicable to all operators
  - It is possible to add qualifying statements to clarify that not all requirements are applicable to all situations and that the operator should enable the type of protection based on their risk assessment for what is applicable to their deployment