Comments on draft-mglt-nvo3-geneve-security-requirements-03

IETF 101, NVO3 WG meeting, London

Ilango Ganga, T. Sridhar

Mar 21, 2018

Comments summary

- Comments posted on the mailing list
  - Theme of comments: focus on potential security threats and requirements to mitigate those threats as applicable to Geneve deployments
  - Not all data centers environments have all possible risks highlighted in the document, some of the risks may not be applicable to certain deployments
  - The objective is to educate the reader on possible risks, for example due to deployment in multi-tenancy environments, and provide options for mitigation, so they can make the right choice as applicable to their specific environments

Some of the outstanding issues being resolved

- Data privacy may be offered as a service by the service provider or a tenant may choose to bring their own data privacy policies
  - So NVE may provide the option to encrypt data packets
  - Existing protocols would suffice for the most part
- Some of stated requirements may not be applicable for Geneve transit devices
  - Reconcile requirements document to be consistent with Geneve architecture
  - Partial encryption, could be addressed with existing mechanisms, requirements should not prescribe a particular solution.
- Requirements related performance optimization are not necessarily to address a threat, for example flow based granularity, partial encryption
- Should we repeat the requirements for multicast use cases? Also multiple unicast tunnels may be used to realize overlay multicast

Next Steps

- We are working with the authors of draft-mglt-nvo3-geneve-security-requirements to resolve the comments to make progress