NV03 Security
Roundtable Discussion
Summary and Next-steps

30-March-2017
Security in the context of NV03

• Neglected.
  • There were two drafts, both have expired.
  • This is a RTG working group, as a result the expertise and focus on security has been limited. We need to do better.
Requirements

• Need to define the context in which NVO3 is operating and what are the relevant assumptions there. Isolation on the tenant and infrastructure namespaces.

• Data plane has converged and needs to be reviewed from security aspects perspective. Need to involve SEC directorate for that.

• Requirements for control plane.

• VNI identifier space.

• Confidentiality of the data plane encapsulation. DTLS option. What does that mean for middleboxes?

• Integrity of the dataplane headers. Applicability of IPsec AH.

• Integrity of the whole NVO3 packet. Applicability of IPsec ESP.

• Multiple nested crypto transforms and their impact on each other and of resulting payload to the middleboxes.

• HW friendliness of MAC and crypto transforms.
Discussion Outcome

• Security aspects are critical.
• Security related drafts need to be resurrected, cleaned up, merged with changes that happened in data plane, and with the outcome of control plane.
• Need to engage SEC-DIR for early reviews.