Security Requirements for NVO3

draft-ietf-nvo3-security-requirements-01

Sam Hartman
Dacheng zhang
Margaret Wasserman

Updates since -00

- Extract requirements from the discussion and list them in bullets. Every requirement is associated with justification and candidate techniques.
- Revise the assumptions of the analysis
- Delete section 4.3 and integrate the contents into the requirements directly
- The security requirements covers the data/control traffics between NVEs and hypervisors, and the data/ control traffics within the NVO3 overlay
- Delete the discussion about the new security challenges brought by the NVO3 architecture in Section 6

Assumptions

- Attacks could come from:
  - Underlying network of the overlay
  - Network connecting NVEs and hypervisors
  - Malicious tenant systems
  - Compromised hypervisors
  - Compromised NVEs
- The compromise of NVA will result in the failure of whole security solution.

Basic Principles

- The tolerance of outside attackers
- The confinement of inside attackers
- The techniques considered:
  - Authentication, Authorization
  - Packet level security protection (integrity, origin authenticity, confidentiality)
  - Key Management (key usage scope)
  - …

Future Work

- Update the introduction to the NOV3 architecture
- Key management requirements needs to be carefully revised.
  - Remove the over strict key requirements
  - Remove the discussion about securing NVE-NVE control traffic, and move the discussions about group keys into the data plane security.
- Discuss the influences to security requirements introduced by different NVO3 network architectures.

- Commnets?