# Security Requirements of NVO3

## draft-ietf-nvo3-security-requirements-02

Sam Hartman
Dacheng Zhang
Margaret Wasserman

IETF 89 London

# Updates Since -01 (1)

- Change the diagram of overlay architecture
- Chang the threat model:
  - Inside attacks: from compromised NVO3 devices
  - Attacks from malicious TSes
  - Outside attacks: from underlying networks
- Clarify the tolerance of compromised NVA is out of scope

# Updates Since -01 (2)

- Add the requirements with NVA-NVA control plane
  - Except the key deployment requirement (REQ 5), all the other requirements in the NVE-NVA control plane (REQs 1,2,3,4, 6, and 7) are applicable in the NVA-NVA control plane as well.
  - The security solution of NVO3 SHOULD be able to provide different keys to protect the unicast control traffics exchanged between different NVAs respectively.
  - If there are multicast packets, the security solution of NVO3 SHOULD be able to assign distinct cryptographic group keys to protect the multicast packets exchanged among the NVAs within different multicast groups.

# Updates Since -01 (3)

- Add section 6 which introduces the techniques which can potentially be used
  - Entity Authentication
  - Packet Level Security
  - Authorization
- Remove the support of AKMP from the requirement list and disucss the related issues in the security considerations

# Updates Since -01 (4)

- Provide a list of the issues not covered
  - How to manage keys/credentials during their life periods
  - How to support algorithm agility
  - How to provide accountability
  - How to secure the management interfaces
  - Use underlying security protocols versus design integrated security extensions

Comments?