# Geneve Security Requirements

**draft-mglt-nvo3-geneve-security-requirements**

**Migault, Boutros, Wings, Krishnan**

# Security Requirements

SEC-OP: Requirements to validate a specific deployment

- intended for operators
- security mechanisms are not specified and could be anything
- Considers deployment specifities, risk analysis
    - may not be applicable

SEC-GEN: Requirements for Geneve Security Mechanism

- Protocol designers
- GSM is TBD (not necessarily a new mechanism)
- Address ANY Geneve deployment compatible with the Geneve architecture

# Security Requirements

SEC-OP and SEC-GEN are two sets of requirements

- Not competing

SEC-OP: How do I say one deployment is secured ?

- Yes if all requirements are matched.

SEC-GEN: Can $M$ be a GSM ?

- Yes if all requirements are matched.

All requirements are matched:

- When none of them raises an issue.
    - SEC-OP may be non applicable

# SEC-OP- Protection against traffic sniffing

- SEC-OP-1: A secure deployment of a Geneve overlay SHOULD by default encrypt the inner payload. A Geneve overlay provider MAY disable this capability for example when encryption is performed by the Tenant System and that level of confidentiality is believed to be sufficient. In order to provide additional protection to traffic already encrypted by the Tenant the Geneve network operator MAY partially encrypt the clear part of the inner payload.

# SEC-OP - Protection against traffic sniffing

- SEC-OP-2: A secure deployment of a Geneve overlay MUST evaluate the information associated to the leakage of the Geneve Outer Header, Geneve Header and Geneve Option. When a risk analysis concludes that the risk of leaking sensitive information is too high, such MUST NOT be transmit in clear text.
- SEC-OP-3: A secure deployment of a Geneve overlay MUST evaluate the risk associated to traffic pattern recognition. When a risk has been identified, traffic pattern recognition MUST be addressed with padding policies as well as generation of dummy packets.

# SEC-OP - Protecting against traffic injection

- SEC-OP-4: A secure deployment of a Geneve overlay SHOULD authenticate communications between NVE to protect the Geneve Overlay infrastructure as well as the Tenants System's communications (Geneve Packet). A Geneve overlay provider MAY disable authentication of the inner packet and delegates it to the Tenant Systems when communications between Tenant's System is secured. This is NOT RECOMMENDED. To prevent injection between virtualized network, it is strongly RECOMMENDED that at least the Geneve Header is authenticated.

# SEC-OP - Protecting against traffic injection

- SEC-OP-5: A secure deployment of a Geneve overlay SHOULD NOT process data prior authentication. If that is not possible, the Geneve overlay provider SHOULD evaluate its impact.

# SEC-OP - Protection against anti-replay

- SEC-OP-6: A secure deployment of a Geneve overlay MUST evaluate the communications subject to replay attacks. Communications that are subject to this attacks MUST be authenticated with an anti replay mechanism. Note that when partial authentication is provided, the part not covered by the authentication remains a surface of attack. It is strongly RECOMMENDED that the Geneve Header is both authenticated with anti replay protection.

# SEC-OP Security Management

- SEC-OP-7: A secure deployment of a Geneve overlay MUST define the security policies that associates the encryption, and authentication associated to each flow between NVEs.
- SEC-OP-8: A secure deployment of a Geneve overlay SHOULD define distinct material for each flow. The cryptographic depends on the nature of the flow (multicast, unicast) as well as on the security mechanism enabled to protect the flow.

# SEC-GEN- Protection against traffic sniffing

- SEC-GEN-1: Geneve security mechanism MUST provide the capability to encrypt the inner payload.
- SEC-GEN-2: Geneve security mechanism SHOULD provide the capability to partially encrypt the inner payload header.
- SEC-GEN-3: Geneve security mechanism MUST provide the capability to encrypt a single or a set of options while leave other Geneve Option in clear. Reversely, a Geneve security mechanism MUST be able to leave a Geneve option in clear, while encrypting the others.

# SEC-GEN- Protection against traffic sniffing

- SEC-GEN-4: Geneve security mechanism MUST provide means to encrypt the information of Geneve Header. Reversely, a Geneve security mechanism MUST be able to leave in clear header information while encrypting the other.
- SEC-GEN-5: Geneve security mechanism MUST provide the ability to pad a Geneve packet.
- SEC-GEN-6: Geneve security mechanism MUST provide the ability to send dummy packets.

# SEC-GEN - Protecting against traffic injection

- SEC-GEN-7: Geneve Security mechanism MUST provide means for a tunnel endpoint (NVE) to authenticate data prior it is being processed. A tunnel endpoint (NVE) MUST be able to authenticate at least:
  - the Geneve Header and a subset of Geneve Options
  - the Geneve Header, a subset of Geneve options and the Geneve inner payload
  - the Geneve Header, a subset of Geneve options and the Geneve inner payload or the portion of the inner payload in case the Tenant's System provides some authentication mechanism.

# SEC-GEN - Protecting against traffic injection

- SEC-GEN-8: Geneve Security mechanism SHOULD provide means for a transit device to authenticate the Geneve Option prior processing it. Authentication MAY concern the whole Geneve packet, but MAY be limited to the Geneve Option.

# SEC-GEN - Protection against anti-replay

- SEC-GEN-10: Geneve Security mechanism MUST provide means for a tunnel endpoint (NVE) to validate the Geneve Header corresponds to the Geneve payload, and discard such packets.

# SEC-GEN Security Management

- SEC-GEN-10: A Geneve security mechanism MUST be managed via security policies associated for each traffic flow to be protected. Geneve overlay provider MUST be able to configure NVEs with different security policies for different flows. A flow MUST be identified at minimum by the Geneve virtual network identifier and the inner IP and transport headers, and optionally additional fields which define a flow (e.g., inner IP DSCP, IPv6 flow id, Geneve options).

# SEC-GEN Security Management

- SEC-GEN-11: A Geneve security mechanism MUST be able to assign different cryptographic keys to protect the unicast tunnels between NVEs respectively.
- SEC-GEN-12: A Geneve security mechanisms, when multicast is used, packets,MUST be able to assign distinct cryptographic group keys to protect the multicast packets exchanged among the NVEs within different multicast groups. Upon receiving a data packet, an egress Geneve NVE MUST be able to verify whether the packet is sent from a proper ingress NVE which is authorized to forward that packet.

**Thanks!**