Geneve Protocol Security Requirements

draft-mglt-nvo3-geneve-security-requirements-01

Security Requirements drafts

The NVO3 working group has two security requirement draft:

1. ENV: draft-ietf-nvo3-security-requirements-07
2. GEN: draft-mglt-nvo3-geneve-security-requirements-02
    a. Working version available on github and early next week version should be published.

While both drafts are focused on security requirements, and present a threat analysis, we believe:

- Their scope is complementary,
- Their requirements are aligned
- There is interest for the WG to publish both documents

ENV vs GEN - Scope

ENV is focused on environment and architecture security requirements

- [...] discusses the security risks that a NVO3 network may encounter and tries to provide a list of essential security requirements that needs to be fulfilled.
- [...] introduces the candidate techniques which could be potentially used to construct a security solution fulfilling the NVO3 security requirements.

GEN is focused on Geneve protocol security requirements

- [...] lists the requirements to protect the Geneve packet components defined in [I-D.ietf-nvo3-geneve] that include the Geneve tunnel IP and UDP header, the Geneve Header, Geneve options, and inner payload.

ENV vs GEN - Scope

ENV and architecture security requirements:

- Have a wider scope:
  - control plane, NVE-NVE data plane, NVE-Hypervisor data plane
- Are not protocol specific.
  - NVE-NVE communication may be protected using different protocols (IPsec, Geneve,...)

GEN and Geneve protocol security requirements:

- Limited to NVE-NVE data plane
- Geneve specific with requirements targeting Geneve Security options

GEN - ENV Alignment

GEN are protocol requirements to achieve ENV architecture requirements

All NVE-NVE Data Plane ENV requirements are covered by GEN requirements

- Version 03 will provide detailed text.
- ENV 1-9, ENV 15-18: out of scope of GEN
- ENV 12 = GEN 13
- ENV 13 = GEN 14
- ENV 10, ENV 11, ENV 14 are achieved differently with GEN 1-16 \ {13, 14}

GEN - ENV Alignment

- ENV 10, ENV 11, ENV 14

REQ 10. The security solution of NVO3 SHOULD be able to provide integrity protection, replay protection, and packet origin authentication for data traffics exchanged between NVEs.

REQ 11. The security solution of NVO3 MAY be able to provide confidentiality protection for data traffics exchanged between NVEs, if information leaking is a concern.

REQ 14. Upon receiving a data packet, an egress NVE MUST be able to verify whether the packet is sent from a proper ingress NVE which is authorized to forward that packet.

Protection Against Traffic Sniffing

GEN-REQ1: The NVE MUST ensure the traffic leaving the NVE has its payload encrypted.

GEN-REQ2: To provide best protection from traffic analysis, the NVE SHOULD encrypt the VM's inner IP address, transport header, and payload.

- Extends R11:
  - Encryption depends on the nature of the payload,
  - Specify the fields that may be encrypted by the NVE when not encrypted by the TS

Protection Against Traffic Injection

GEN-REQ3: A Geneve NVE MUST be able to authenticate the Geneve tunnel Header, and/or the Geneve base header, and/or the immutable Geneve Options, and/or the Geneve payload.

GEN-REQ4: A Geneve NVE MAY be able to authenticate only a portion of the Geneve payload if the Tenant's system is protecting its communication.

GEN-REQ5: A GTN MAY be able to validate the authentication before the packet reaches the Geneve destination NVE.

GEN-REQ6: A GTN MUST be able to insert an authenticated Geneve Option into a authenticated Geneve Packet - protected by the source Geneve NVE.

Protection Against Traffic Injection

GEN-REQ7: A GTN MUST be capable of forwarding the Geneve authenticated packet as an non-authenticated Geneve Packet.

GEN-REQ8: A Geneve NVE SHOULD be able to set different security policies for different flows. These flows MUST be identified from the Geneve Header and/or Geneve Options as well as some inner traffic selectors.

GEN-REQ9: In the case when Tenant systems secure their communications using protocols such as TLS or IPsec. A Geneve NVE MAY be able to selectively encrypt and/or authenticate only the sections that are not encrypted / authenticated by the Tenant System. For example, only the IP, transport (TCP / UDP) in case of TLS/DTLS MAY be encrypted/authenticated, while only the IP header and ESP header MAY be encrypted/authenticated.

Protection Against Traffic Injection

Extends R10 to Geneve by specifying the properties of Geneve authentication mechanism:

- Different combination of the fields in a Geneve packet that need to be authenticated
- How (partial) authentication of the Geneve payload may be achieved and how authentication is shared between the NVE and the TS.
- The necessity to have flow based security policies.
- Properties of authentication mechanism for Geneve Transit Nodes
- Properties regarding Geneve Options

Protection Against Traffic Redirection

GEN-REQ10: A Geneve NVE MUST be able encrypt Geneve base Header, and / or Geneve Payload and/or Geneve Options not intended for the GTN.

GEN-REQ11: A Geneve NVE MAY be able encrypt portion of Geneve Payload as well as as Geneve Options not intended for the GTN.

GEN-REQ12: A transit underlay intermediary node MUST be able to insert an encrypted Geneve Option into an encrypted/ authenticated Geneve Packet - protected by the source Geneve NVE.

GEN-REQ13: A Geneve NVE SHOULD be able to assign different cryptographic keys to protect the unicast tunnels between NVEs respectively.

Protection Against Traffic Redirection

GEN-REQ14: If there are multicast packets, a Geneve NVE SHOULD 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.

Protection Against Traffic Redirection

Extends R11 to Geneve by specifying the properties of Geneve encryption:

- Different combination of the fields in a Geneve packet that need to be encrypted
- How (partial) encryption of the Geneve payload may be achieved and how encryption is shared between the NVE and the TS.
- The necessity to have flow based security policies.
- Properties of encryption mechanism for Geneve Transit Nodes
- Properties of encryption mechanism regarding Geneve Options

Protection Against Anti-Replay

GEN-REQ15: A Geneve NVE or a GTN SHOULD be able to validate the Geneve Header corresponds to the Geneve payload, and discard such packets.

GEN-REQ16: A Geneve NVE or a GTN SHOULD provide anti replay mechanisms and discard replayed packet.

Extends R10, 14, by specifying :

- Properties of the anti replay with Geneve Transit Nodes.

Thanks!