Geneve Security Requirements

draft-mglt-nvo3-geneve-security-requirements-00

Migault IETF99

Why 4 drafts ?

draft-mglt-nvo3-geneve-security-requirements-00

- Security Analysis of Geneve Overlay Network
- Provide requirements to design Geneve Security Options
- Does not provide security recommendations on how to secure Geneve deployment

Protocol Security Requirements

```
    Tenant System    (Other Tenant Systems)    Tenant System
             |                                       |
-------------|---------------------------------------|------------
    G  O  +------+                                +------+
    E  V  | NVE |                                 | NVE |
    N  E  +------+                                +------+
    E  R     ||         Geneve Forwarding Elements       ||
    V  L     ||                                      ||
    E  A   +-----+   +-----+   +-----+   +-----+       +-----+
    Y      |    |====|    |====|    |====|    |====|    |
           +-----+       +-----+   +-----+   +-----+   +-----+
------------------------------------------------------------------

         +--------------------------------------------+
         |      Infrastructure (Hardware, VM)         |
         |                                            |
         +--------------------------------------------+
```

Security Goals

Tenant Isolation: Isolate Tenant Systems within each Virtual Network

- Prevent traffic injection from outside the VN,
- Prevent traffic redirection (passive monitoring)
- Protect Tenant to Tenant communications

Overlay Network Robustness: Make the Geneve robust to attacks, misconfigurations

- Replay attack
- Traffic modification targeting Tenant Systems as well as Geneve infrastructure

Infrastructure Isolation: Isolate the Overlay from underlying infrastructure

Tenant Isolation: Traffic Injection

Tenant’s System may protect their communication with IPsec/TLS

- Such protection is outside the scope of Geneve
- Traffic may still be steered in the VN

The attack is traffic injection from any node (except legitimate NVEs)

- Geneve Header MUST be read by all Geneve elements on path.
- The destination MUST be able to authenticate the incoming packet.
    - Authentication may be limited to the Geneve Header
    - Authentication MUST not impact processing for on path Geneve Elements

Tenant Isolation: Traffic Injection

- REQ1: A Geneve NVE MUST be able to authenticate the Geneve Header including the immutable Geneve Options.
- REQ2: A Geneve NVE MUST be able to agree that authentication includes or not the Geneve Payload, and if so it SHOULD also be able to indicate that only a portion of it is authenticated.
    - Authentication of Geneve Header and Geneve Option does not protect the Geneve Payload
    - Geneve Payload MAY be composed of protected and unprotected part (TLS/IPsec/ESP)
        - Geneve MAY cover the unprotected part, protected part is left to the Tenant
        - Geneve MAY cover the whole Geneve Payload, in which case Geneve Guarantee its delivery is fine.
- REQ3: A Geneve intermediary forwarding element MAY be able to validate the authentication before the packet reaches the NVE.
- REQ4: A Geneve intermediary forwarding element MUST be able to insert an authenticated Geneve Option into an authenticated Geneve Packet.

Tenant Isolation: Traffic Injection

- REQ5: A Geneve intermediary forwarding element not supporting authentication MUST NOT be impacted by the authentication of the Geneve Packet and should be able to handle the Geneve Packet as an non-authenticated Geneve Packet.
- REQ6a: A Geneve NVE SHOULD be able to set different security policies to different flows.
- REQ6b: Geneve secured flows MUST be characterized from the Geneve Header and Geneve Options as well as some inner traffic selectors.
    - Typically an NVE SHOULD be able to selectively encrypt only the sections that are not encrypted by the Tenant System.

Tenant Isolation: Traffic Redirection

The attack is traffic being redirected for passive monitoring, and then reinjected.

- Injection of a modified packet is addressed by traffic injection
- Leakage cannot be prevented by the protocol, it is an environment issue
    - Geneve can prevent revealing information to the attacker.

The information can be:

- Geneve Payload even IPsec/TLS protection by Tenants reveals MAC, IP, (port)
- Geneve Header and Geneve Options

Tenant Isolation: Traffic Redirection

- REQ7: A Geneve NVE MUST be able to agree that the Geneve Payload or portion of it is encrypted as well as as immutable Geneve Options not intended for the intermediary Geneve nodes.
- REQ8 (removed identical as REQ4)
- REQ9: A Geneve intermediary forwarding element MUST be able to insert an encrypted Geneve Option into an encrypted Geneve Packet - protected by the source Geneve NVE.
- REQ10: A Geneve intermediary forwarding element not supporting encryption MUST NOT be impacted by the encryption of the Geneve Packet and should be able to handle the Geneve Packet as an non-protected Geneve Packet.

Overlay Network Robustness

Tenant isolation does not provide anti-replay protection by a rogue Geneve forwarding Element

- An attacker may perform a volumetric attack
  - on the overlay network by overloading or disruption flow engineering (OAM, options)
  - replaying a traffic to tenant systems
- An attacker may also replay an authenticated Geneve Header with crafted Geneve Payload to target an application for example

The following requirements apply:

- REQ11: Geneve Header SHOULD be bound to the forwarded payload. By reading the Geneve Header and the Payload.
- REQ12: Geneve SHOULD be provided anti replay mechanisms.

Infrastructure Isolation

Infrastructure should be isolated from:

- Tenants Communications
- Overlay Network Architecture

Tenants encrypt their communications

Thanks!