Geneve Header Authentication and Encryption Option

draft-mglt-nvo3-geneve-authentication-option-00
draft-mglt-nvo3-geneve-encryption-option-00

Migault IETF99

IPsec/DTLS ?

Can we use existing protocols ?

- UDP encapsulation makes DTLS a “natural candidate”
- Securing tunneled packets makes also IPsec a “potential candidate”

None of these protocol completely fulfill the security requirements for Geneve

- IPsec-like solution seems more adapted
- All proposals are currently based on IPsec [GAO] [GEO][gIPSEC]

[GAO] draft-mglt-nvo3-geneve-authentication-option-00
[GEO] draft-mglt-nvo3-geneve-encryption-option-00
[gIPSEC] draft-boutros-nvo3-ipsec-over-geneve-00

Why not DTLS

Current DTLS 1.3 does not provides authentication only.

- Authentication-only is needed for the Geneve Header to avoid injection

DTLS comes with a key-exchange protocol

- Key exchange may not match Geneve deployment based on forwarding rules controlled by the orchestrator.

Geneve does not provides means to indicate a packet is DTLS-protected or not.

- Different port may be used / defined for Geneve and Geneve”s”

Why not DTLS

DTLS protection is currently not based on traffic policies

- Requested by the DTLS client forced by the DTLS server
- All or none

DTLS protects the whole UDP packet

- Prevents on path modification of the Geneve Header
- There is no need to protect the whole packet
    - In some cases the Geneve Header may be sufficient

Why not IPsec

IPsec/AH authenticate the packet including the outer IP header

- NVE destination cannot be changed
  - Removes the role of Geneve forwarding elements

IPsec/ESP protects the IP payload

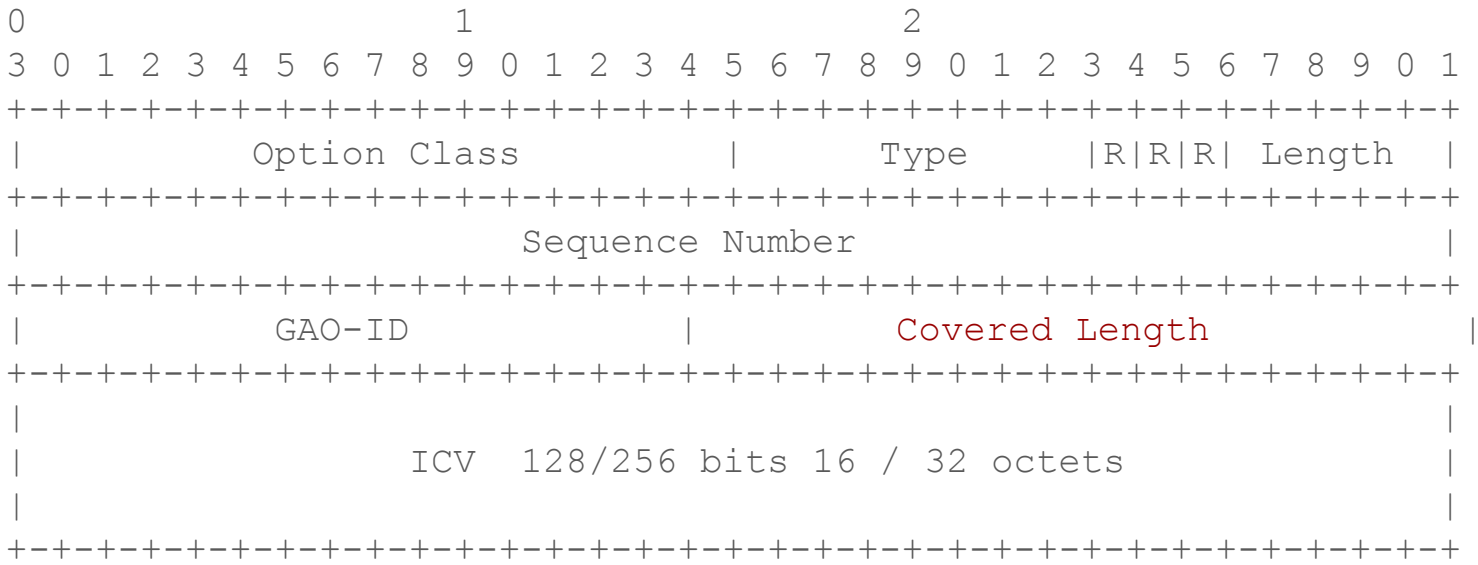
- Authentication-only prevents the Geneve Header to be updated
- Encryption prevents Geneve forwarding elements to update the packet.
  - Removes the role of Geneve forwarding elements
- In some deployment protection does not concern the whole Geneve Packet
  - In some cases the Geneve Header may be sufficient

GAO

Designed principles:

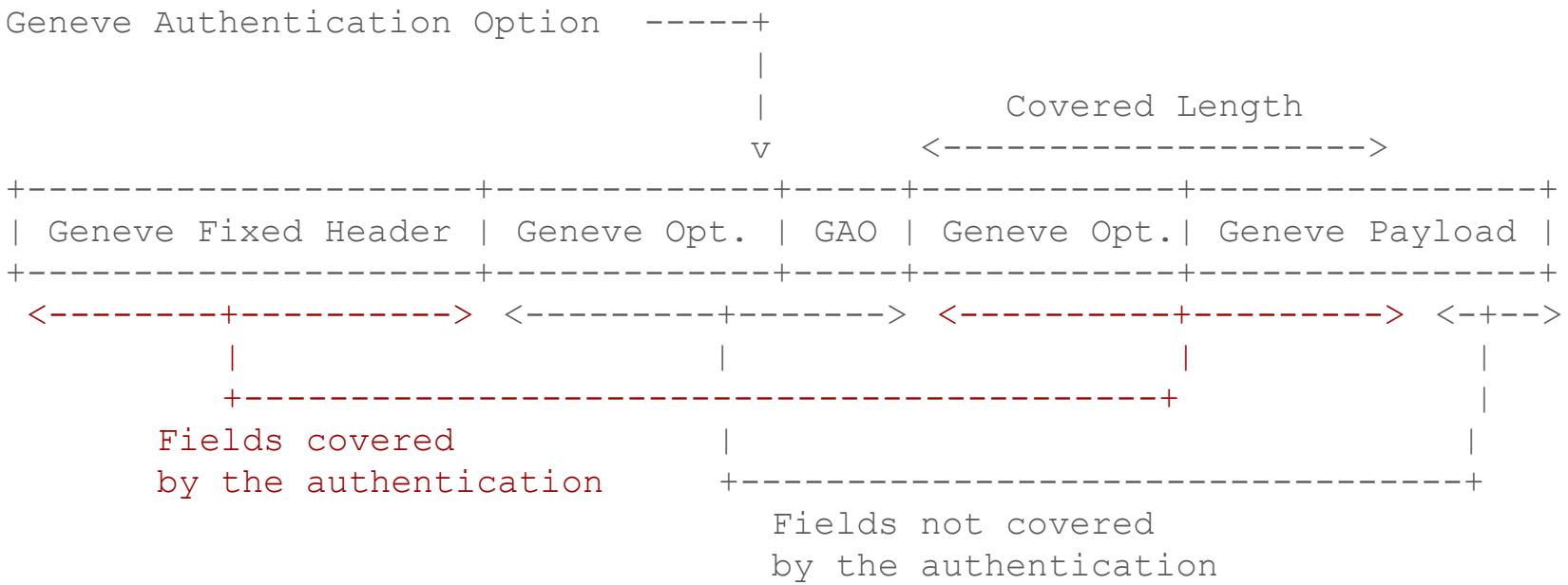
- Inspired by IPsec/AH
  - Anti-replay
  - authentication
- Adapted to Geneve
  - Geneve Option - limited to Geneve Packet (Geneve Header + Geneve Payload, not UDP or outer IPs)
  - Enable the authentication to the Geneve Fixed Header and subset of options.
  - Does not impact processing of the Geneve forwarding elements
  - Possible for Geneve forwarding elements to add their own GAO (for ex to authenticate a given option)

GAO description



- Option Class: 0x0000, Type C unset,
- AUTH_HMAC_SHA2_512_256, AUTH_HMAC_SHA2_256_128.

GAO Placement



GAO Processing

Processing is similar to IPsec/AH some difference:

Covered Length is generated on a per packet basis for outbound traffic

GAO-ID is 16 bit but is associated to a VNI

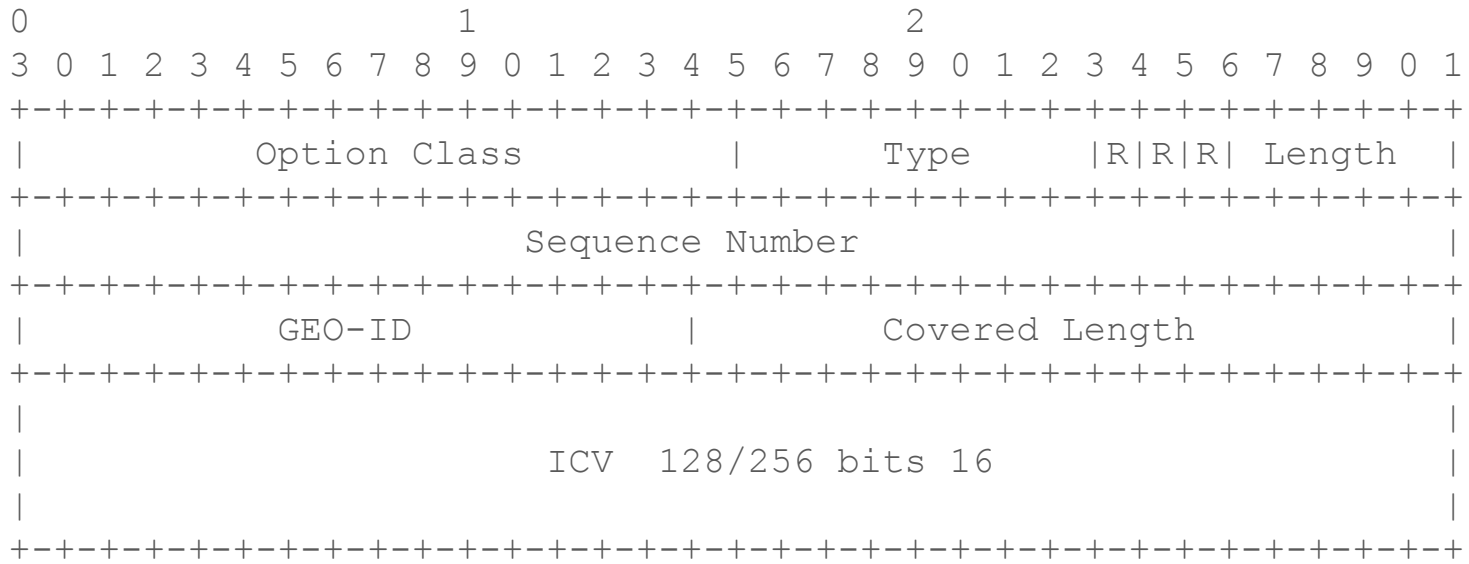
GEO

Follows the same principle design as GAO.

The encrypted payload is not contained into the Geneve Option

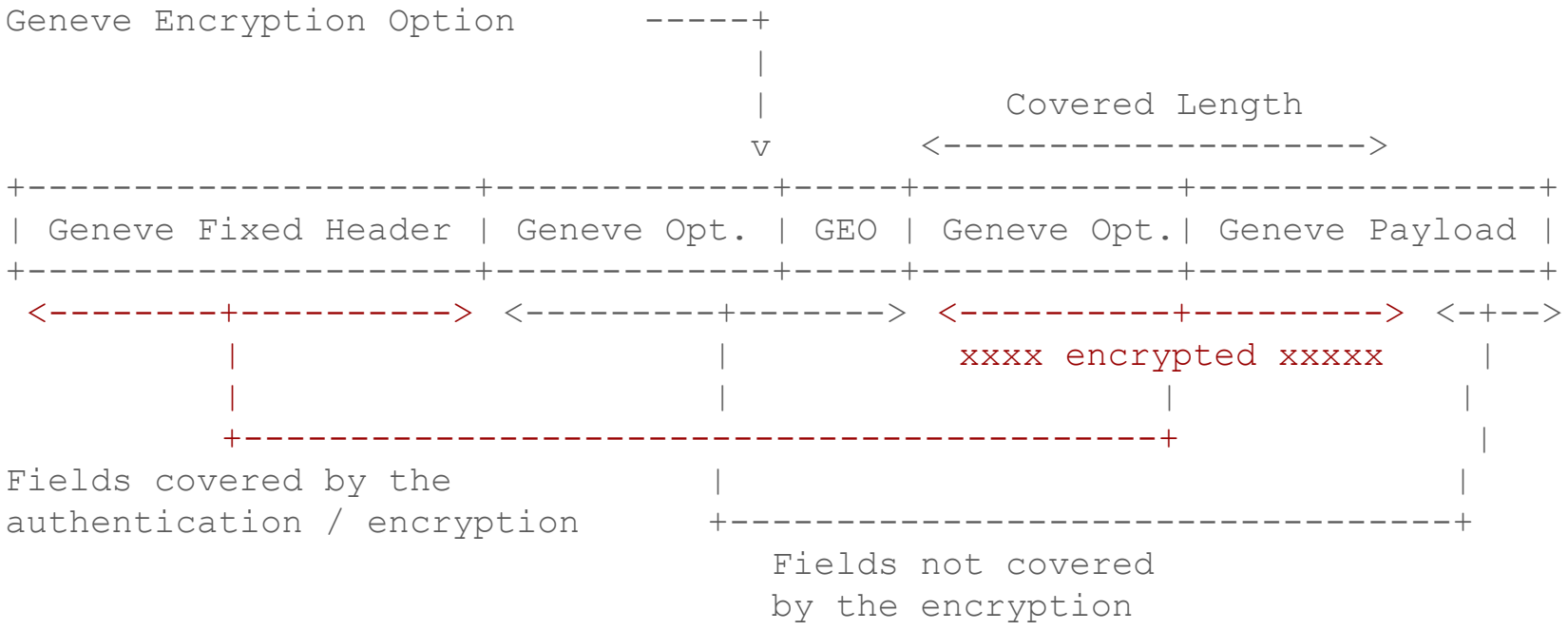
- Length option is coded on 5 bits
- MUST be a terminal Geneve Option. GEO

GEO Description



ENCR_AES_GCM_16, ENCR_CHACHA20_POLY1305.

GEO Placement



GAO / GEO vs gIPsec

- Both are based on IPsec
- Both modify IPsec and thus needs (slight) update to IPsec:
  - SA, SP, IKEv2,....

Differences:

- GEO/GAO uses an Geneve Option to signal the protected segment
  - This signaling can be read from the packet
- gIPsec uses the Protocol field in the Geneve Header to signal a protected Payload.
  - Covered length, covered Geneve Option needs to be agreed by NVEs