Encrypted ESP Ping

draft-antony-ipsecme-encrypted-esp-ping

Antony Antony <antony.antony@secunet.com>

27/07/24

IPsec Background

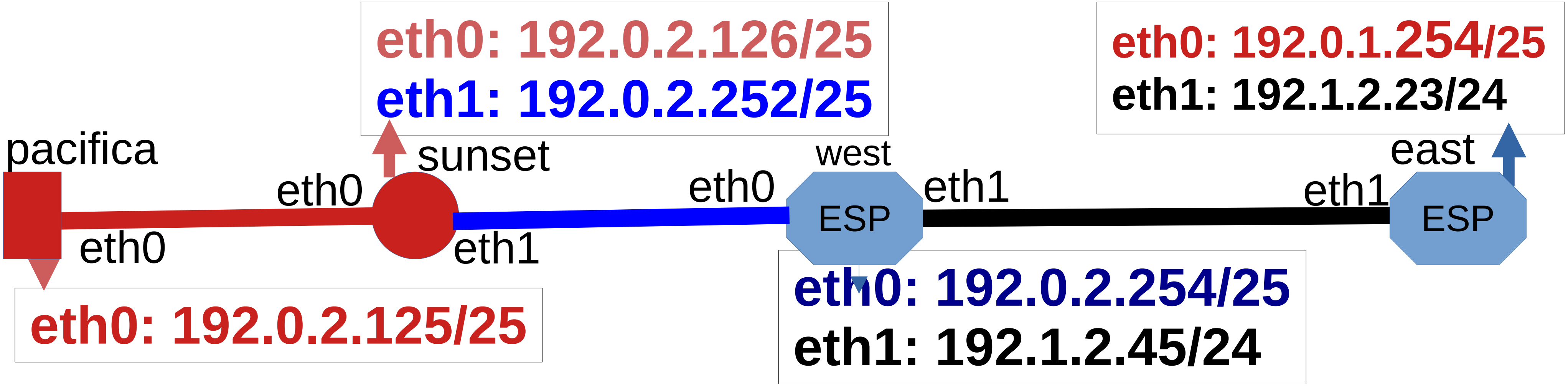
- IKE is control plane (UDP 500 or UDP 4500)
- ESP is Data plane (ESP or ESP-in-UDP 4500)

Problem Statement

- Diagnose ESP after IKE is established
- ESP packets do not share fate with IKE
- IKE might succeed but ESP packets are dropped
- Hard to detect and recover
- Data traffic is blackholed
- Why Not Use Existing IP Tools?

Why not ping over IPsec?

IPsec gateways has no IP from policy



eth0: 192.0.2.126/25
eth1: 192.0.2.252/25

eth0: 192.0.1.254/25
eth1: 192.1.2.23/24

pacifica
eth0
eth0: 192.0.2.125/25

sunset
eth0
eth1

west
eth0
ESP
eth1
eth0: 192.0.2.254/25
eth1: 192.1.2.45/24

east
eth1
ESP

```
xfrm policy 192.0.2.125/25  <-> 192.0.2.125/25
xfrm state  192.1.2.23 <=> 192.1.2.23 SPI 0xAABBCCDD
```

espping -s 0xAABBCCDD -I 192.1.2.45 192.1.2.23

Use cases

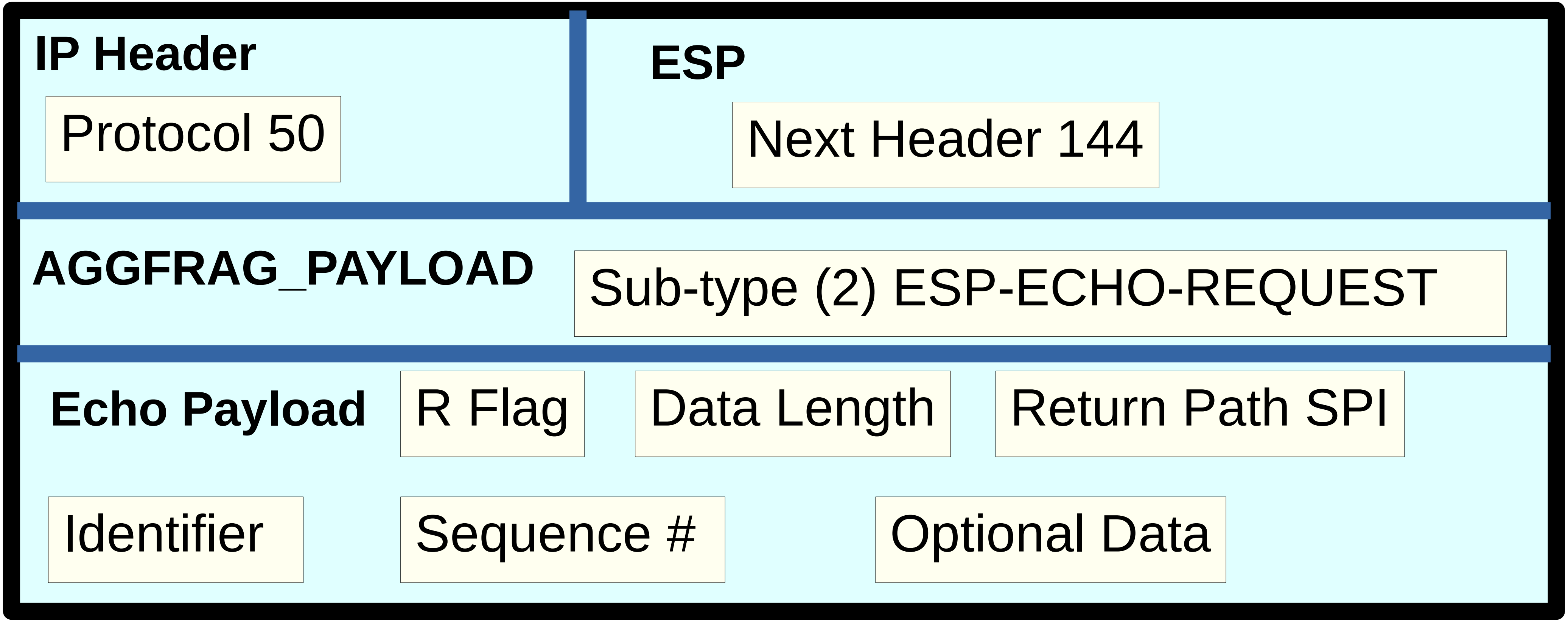
- Diagnose ESP Blocked or Filtered
- Probing Multiple ESP Paths to same end point
- Probe Return Path
  - ESP is two unidirectional Security Associations

Example

- espping -s <size> -I <src ip> [--spi <spi>] <dst ip>

- espping -I 192.1.2.23 –spi 0xAABBCCDD 192.1.2.45

Packet format : Request



IP Header

Protocol 50

ESP

Next Header 144

AGGFRAG_PAYLOAD

Sub-type (2) ESP-ECHO-REQUEST

Echo Payload

R Flag

Data Length

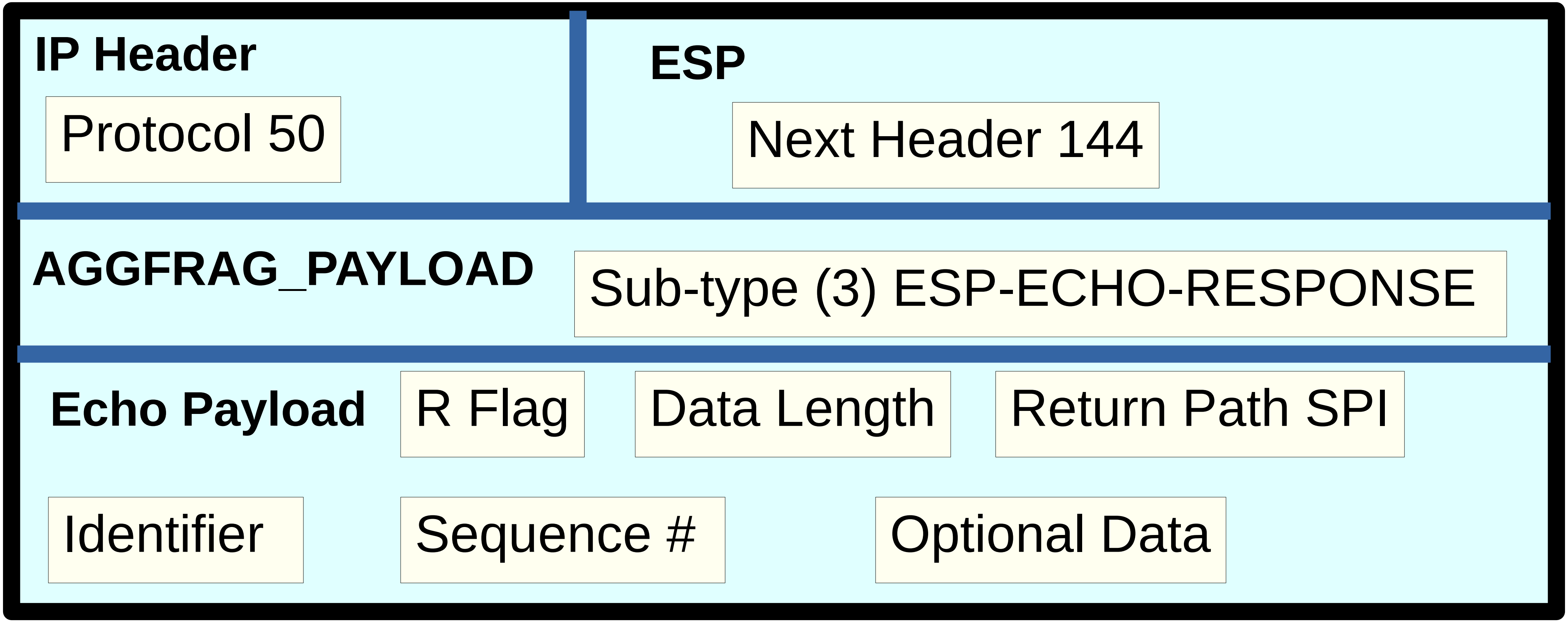
Return Path SPI

Identifier

Sequence #

Optional Data

Packet format : Response



IP Header

Protocol 50

ESP

Next Header 144

AGGFRAG_PAYLOAD

Sub-type (3) ESP-ECHO-RESPONSE

Echo Payload

R Flag

Data Length

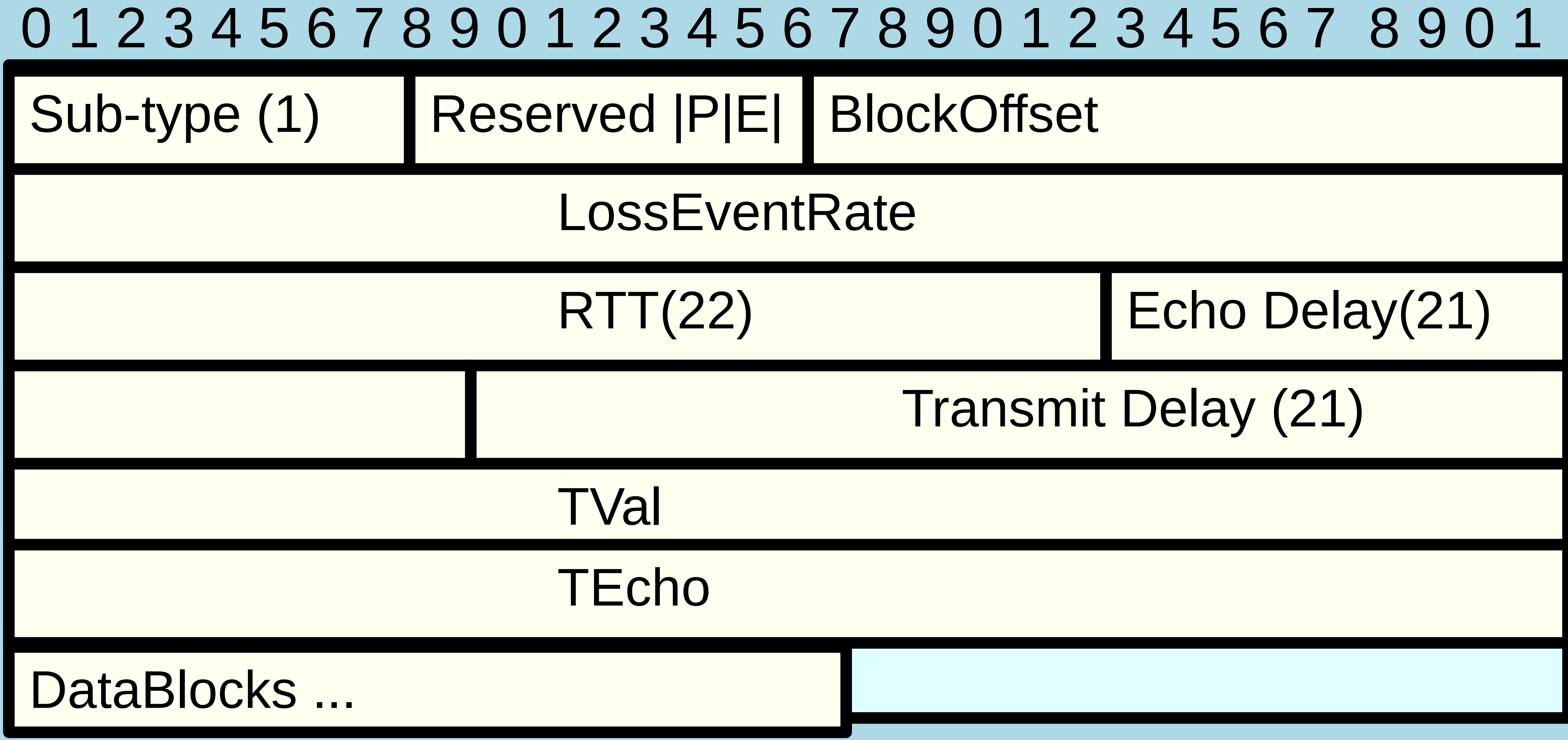
Return Path SPI

Identifier

Sequence #

Optional Data

RFC 9347 CC Payload



0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1

Sub-type (1) | Reserved |P|E| | BlockOffset

LossEventRate

RTT(22) | Echo Delay(21)

Transmit Delay (21)

TVal

TEcho

DataBlocks ...

IP-TFC Congestion Control Payload

- CC payload helps to discover path properties:
  - One way delays,

  - loss rate.

  - estimated bandwidth
- Useful to probe manually even when IP-TFS is not negotiated

IKEv2 Notify to announce support

Add IKEv2 Notification in -03 I.D.

ENCRYPTED_PING_SUPPORTED

SADB Implementation on receiver

- How to validate Return Path requested?
  - SADB is unidirectional
  - Especially when there are multiple SAs
  - Only IKEd knows the return path in its peer DB

  - Respond only to Paired SA?
  - Respond to all SA between same peer ?
    - Think of Fiber and Satellite backup path

Questions / Feedback?

Adoption?

Linux implementation

Linux: ESP Ping Socket (similar to ICMP ping socket)

Encrypted ESP Ping socket

- IPPROTO_ESPPING:
- Send the payload and receive response.
  - Validate destination IP + SPI
  - Validate return source address + Return SPI

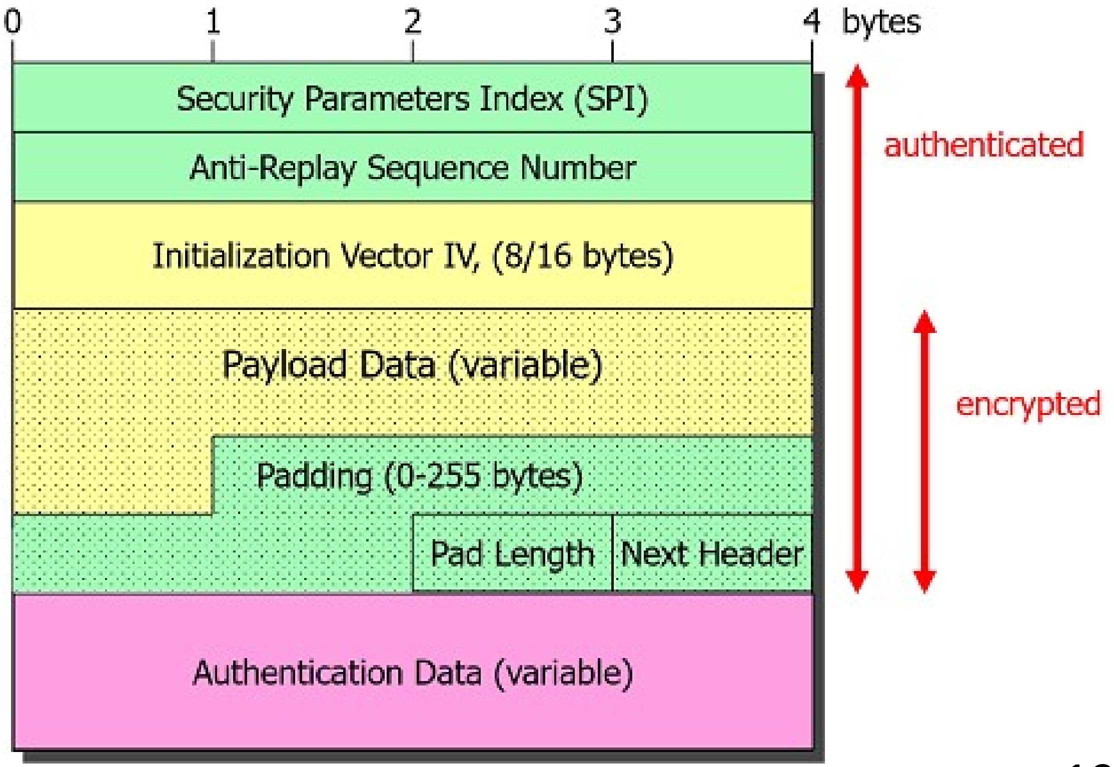
Implementation : Linux SADB?

- How to validate Return Path using SADB?
  - SADB is unidirectional
  - Simple a pair of SA is easy
  - Multiple SA between same pair (doable using peer DB)
  - SA over LTE and WiFi (may need external Daemon/IKEd)
- Sockets : Return response from other SPI
  - Based in Identifier in the payload, meta data (TTL, SPI,..)

Similar ideas

- MPLS LSP ping with return path : RFC 7110
- Bidirectional Forwarding Detection (BFD)
  - IP only (Not suitable for Encrypted ESP Ping)
  - https://www.rfc-editor.org/rfc/rfc8562

ESP Message


0
1
2
3
4
bytes
Security Parameters Index (SPI)
Anti-Replay Sequence Number
Initialization Vector IV, (8/16 bytes)
Payload Data (variable)
Padding (0-255 bytes)
Pad Length
Next Header
Authentication Data (variable)
authenticated
encrypted