

ESP Problem Statement

draft-mrossberg-ipsecme-multiple-sequence-counters-01

Steffen Klassert

ESP problems in today's networks

- Replay protection and packet reordering
 - Lot of proposals to fix this
 - IETF 117
- Header and Trailer format
 - Might not fit anymore to all today's usecases
 - TODAY

Header and Trailer format

Problematic scenarios

- High-Speed Links
 - Header and trailer may end up in different cachelines
 - ESP encrypted payload alignment too short
- Software-Defined Networking (SDN)
 - Uses information from the inner transport header (ESP encrypted)

Possible solutions (High-Speed Links)

- Header and trailer may end up in different cachelines
 - Move trailer fields to the header
- ESP encrypted payload alignment too short
 - Adjusting alignment requirements to 16 or 32-byte (SMID, AVX)

Move trailer fields to the header

■ Advantages:

- Software packet processing benefits from cache locality
- Parsing is simpler, no variable-length payload in between

■ Disadvantages:

- Larger change to the existing packet layout

Adjusting the alignment requirements

- Advantages:
 - SMID and AVX instructions operate faster
- Disadvantages:
 - Trailer might still not be aligned for SMID or AVX
 - Packets require more padding to align the trailer

» **Usefull if the trailer is removed too.**

Possible solutions (SDN)

- Uses information from the inner transport header (ESP encrypted)
 - Use an encryption offset
 - Move the ESP header between transport header and payload

Use an encryption offset

■ Advantages:

- Enables SDN usecases
- Is optional (offset zero means encrypt everything)

■ Disadvantages:

- Intermediate devices need to implement ESP to parse the header.



Google PSP uses that approach!

Move ESP between transport header and payload

■ Advantages:

- Transparent for intermediate devices

■ Disadvantages:

- Significant change due to layering violation

» **Not recommended!**

Which way to solve the problems?

- Adjust the ESP protocol
- Define a new protocol
- Update the WESP protocol (not considered in the draft)

Adjust the ESP protocol

- Works to fix the sequence number problems
 - Some header fields interpreted differently
 - No change to header trailer format
- Problematic when changing header trailer format
 - No new protocol number
 - New version needs to be negotiated
 - Not transparent for middleboxes
 - SDN case does not work

Define a new protocol

- Works for sequence number problems and format change
- Maybe Google PSP + sequence number field
- Most invasive change
- Most flexible change

Update WESP protocol

- Works for sequence number problems and format change
- Not widely used
- But abuse of the original intend of WESP
- Has a version number field (2-bit)
 - Current version is 0
 - Header/trailer can be adjusted
 - Transparent to middle boxes
 - SDN case will work

Questions, suggestions?
WG adoption?

