

# ESP Problem Statement

draft-mrossberg-ipsecme-multiple-sequence-counters-00

Steffen Klassert

# ESP problems in today's networks

- Replay protection and packet reordering
  - Lot of proposals to fix this
  - Discussed in:  
`draft-mrossberg-ipsecme-multiple-sequence-counters-00`
- Header and Trailer format
  - Might not fit anymore to all today's usecases
  - Still TODO in the draft

# Replay protection and packet reordering

# Problematic scenarios

- Multicore Software Processing
  - Needs synchronization between CPUs
  - Introduces reorder
- QoS support
  - Introduces reorder (intentional)
- Multipath
  - Introduces reorder
- Multicast
  - Needs synchronization between multiple senders
  - Introduces reorder

# Possible solutions

1. Disabling replay protection
2. Increase anti-replay window sizes
3. Multiple IKE SAs
4. Multiple child SAs
5. sub-child SAs

# Disabling replay protection

## ■ Advantages:

- solves all the reordering and synchronization issues
- No change in the standards needed

## ■ Disadvantages:

- Significantly lowers the level of security
- Receive side can't parallelize over multiple CPU cores

# Disabling replay protection

- Solves:
  - Multicast
  - Multipath
  - QoS
- Does not solve:
  - Multicore
    - Solves just the transmit side problems
- But: Significantly lowers the level of security!

» **Not a solution for the general case!**

# Increase anti-replay window size

## ■ Advantages:

- No change in the standards needed

## ■ Disadvantages:

- Needs synchronization (CPU cores / multicast senders)
- Receive side can't parallelize over multiple CPU cores
- Anti-replay windows can't grow indefinitely large
- Complex configuration (which size fits for a given usecase?)

# Increase anti-replay window size

- Solves:
  - (Multipath)
  - (QoS)
- Does not solve:
  - Multicore
  - Multicast

» **Not a solution for the general case!**

# Multiple IKE SAs

## ■ Advantages:

- No changes to existing standards required
- Independent sequence numbers and anti-replay windows
- Distinct SPIs allow RX side RSS or explicit steering

## ■ Disadvantages:

- Negotiation (time and communication) overhead
- state/memory overhead
- Unspecified failure model if a subset of SAs can't be established

# Multiple IKE SAs

- Solves:
  - Multicore
  - Multicast
  - Multipath
  - QoS
- Does not solve:
  - Combinations of different cases (e.g. Multicore + QoS)
- But: Has scalability issues

» **Not a solution for the general case!**

# Multiple child SAs

## ■ Advantages:

- Just minor changes to existing standards required
- Independent sequence numbers and anti-replay windows
- Distinct SPIs allow RX side RSS or explicit steering

## ■ Disadvantages:

- Negotiation (time and communication) overhead
  - Much less than ,multiple IKE SAs'
- state/memory overhead
  - Much less than ,multiple IKE SAs'
- Unspecified failure model if a subset of SAs can't be established

# Multiple child SAs

- Solves:
  - Multicore → (draft-ietf-ipsecme-multi-sa-performance-01)
  - Multicast
  - Multipath
  - QoS
- Does not solve:
  - Combinations of different cases (e.g. Multicore + QoS)
- But: Still does not solve the generic case

» **Low hanging fruit, can solve a lot of usecases!**

# Multiple sub-child SAs

- Idea: Use multiple sequence counters per child SA
- Encode the sequence number counter ID on some header field
- Multiple possibilities to achieve this
  - Not (yet) clear which one is the best

# Multiple sub-child SAs

- Use bits of the sequence number
  - Draft-ponchon-ipsecme-anti-replay-subspaces-00
  - Reduces available sequence numbers per sub-child SA (ESN only)
  - Limited RSS support in current NICs
- Use some bits of the SPI
  - RSS support in current NICs
- Use a new header field
  - Draft-ponchon-ipsecme-anti-replay-subspaces-02
    - Transmit 64 bit sequence number
  - Biggest change to current standards
  - Limited RSS support in current NICs

# Multiple sub-child SAs

## ■ Advantages:

- Independent sequence numbers and anti-replay windows
- Distinct SPIs allow RX side RSS or explicit steering
- No rekeying overhead
- Clean failure model

## ■ Disadvantages:

- Most complex change
- Needs care to avoid security implications
  - IVs must not repeat for counter modes
  - Rekey, byte, packet limits must apply to all sub-SAs combined

# Multiple sub-child SAs

- Solves:
  - Multicore
  - Multicast
  - Multipath
  - QoS
  - Combinations of different cases (e.g. Multicore + QoS)
- But: Most complex change, has security implications
- Need to choose a header field: SPI, sequence number, new field

» **Might solve the general case!**

# Header and Trailer format

# Header and Trailer format

- Still TODO in the draft
- Need to identify usecases for different formats:
  - Google published PSP for HW offloads
  - Some discussion at IETF 108

Is the WG interested to continue this work?

