IPsec and IKE anti-replay subspaces

draft-ponchon-ipsecme-anti-replay-subspaces-03

Paul Ponchon, Mohsin Shaikh, Hadi Dernaika, Pierre Pfister, Guillaume Solignac

Presenting today

IPsecme - IETF 118 - Nov 9th 2023

Quick Recap

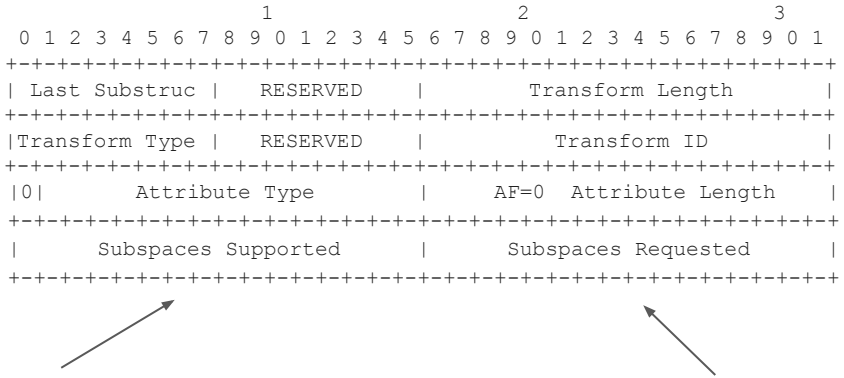
- Anti-replay protection issues with multi-path, QoS, multi-core, multicast
  - draft-mrossberg-ipsecme-multiple-sequence-counters-01

- Alternative solution is to allocate multiple SAs
  - draft-ietf-ipsecme-multi-sa-performance-02
  - Our problem is that this would create a *ton* of SAs
    - Many more keys, many more IKE messages
      - IKEv2 was designed to reduce the number of messages
      - PFS will drain resources

- Our Solution TLDR:
  - Cutting down 64 bits anti-replay sequence number into N subspaces.
  - This is an anti-replay issue, let’s fix anti-replay
    - Single SA, single RTT, all subspaces allocated at once
    - No violation of traffic selector rules. Keep change minimal in IKE.

IKE extension for Sequence-Number Subspaces (SNS) support

- Introducing the SNS Transform to ESP proposal
  - Similar to other negotiated crypto parameters, like ENCR, PRF, ESN, …



Supported inbound subspaces

Requested outbound subspaces

SNS Implementation status

- ESP with subspaces Implemented in VPP.
  - Currently working on clean-up for open-sourcing

- IKE negotiation implemented in Strongswan
  - connections.<conn>.children.<child>.esp_proposals=<esp-proposal>-snsX_Y
  - E.g. **aes128-sha256-sns16_4** indicates we support max 16 inbound subspaces and are requesting for 4 outbound subspaces.

- Meraki (closed-source) implementation
  - Targeting deployment in Cisco Meraki SD-WAN routers next year.
  - How we use subspaces:
    - **Outbound:** Per core **x** Per path (per local uplink x per remote uplink)
    - **Inbound:** Subspaces distributed across cores

Draft Status

IPRs:

- 2 IPRs disclosed with good terms
- Rumors of another patent. No-one was able to find it…

Overall discussions over last 3 IETFs

- 3 people* expressed support for adoption.
- 3 people* supportive of the work and facing similar challenges.
- 1 person expressed concerns during IETF 115, but silence since then.

How much longer are we going to have to wait to have an adoption call ?

* from different companies, excluding co-authors