Anti-replay sequence number subspaces

draft-ponchon-ipsecme-anti-replay-subspaces

Mohsin Shaikh (presenter), Paul Ponchon, Hadi Dernaika,
Pierre Pfister, Guillaume Solignac
IETF 117 @ San Francisco

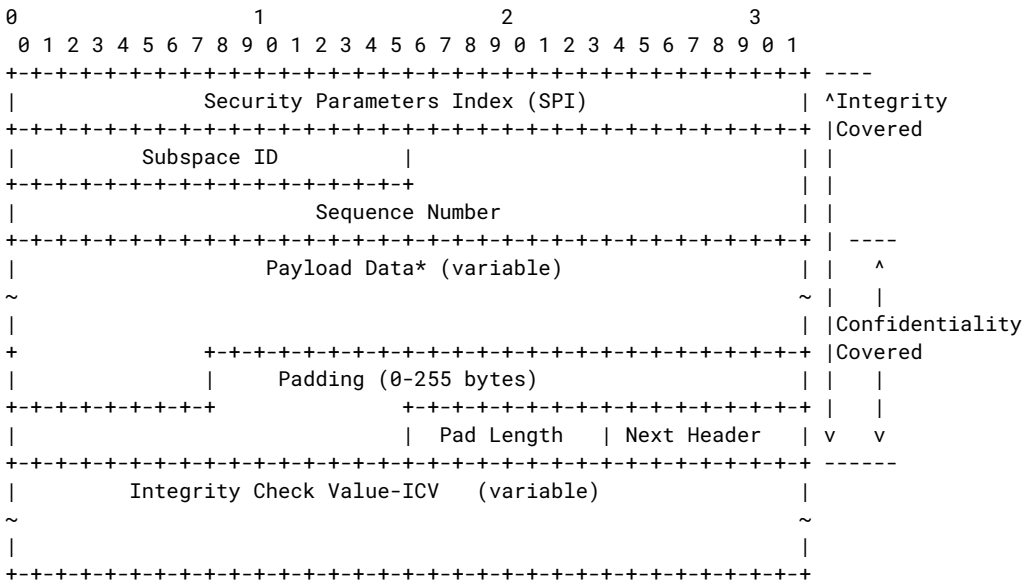
Quick Recap

- Proposal to use multiple sequence number subspaces as an alternative to creating multiple child SAs for multi-core performance
- Additionally support QoS and traffic engineered paths
- In draft-ponchon-ipsecme-anti-replay-subspaces-01 we added IKE transform to negotiate max number of subspaces
- We also increased the sequence number field in ESP packet to 64-bits with subspace ID stored in most significant 16 bits

Implementation

- We are working on implementing this in VPP open-source data-plane (https://fd.io)
- We are also working on a closed source implementation intended for deployment in Cisco Meraki’s devices in the coming months

Updates in draft-02 since IETF 116



- The subspace ID must be between 0 to “N-1” where “N” is the max number of subspaces negotiated by IKE.
- ESN negotiation must be disabled as negotiating subspaces implies a 16-bit subspace ID and 48-bit sequence number counter.

Updates in draft-02 since IETF 116 (contd.)

- The 48-bit sequence number counter must not be allowed to cycle. A 1 Tbps would exhaust a subspace in over 938 hours (39 days). Assuming ethernet frames of 1500 bytes, T = 2^48 (pkts) * 1500 (B/pkt) * 8 / 10^12 (bps) = ~3.4 * 10^6 seconds = ~938 hours.
- ICV calculation begins from start of ESP SPI field to end of ESP payload.
- IPR disclosure from Cisco Systems

- We support draft-mrossberg-ipsecme-multiple-sequence-counters being presented today which discusses using multiple sequence number counters
- We also welcome any support on the mailing list or in person
- We intend to deploy this on Cisco Meraki's ~2 million (and growing) devices worldwide
- Should the working group work to adopt and help us deploy a standard or should this remain a draft based extension?

Q&A