ChaCha20+Poly1305 for IPsec

Yoav Nir

IETF 89
draft-nir-ipsecme-chacha20-poly1305

What is this draft?

- Describes the use of ChaCha20 as a cipher for ESP
- Describes the use of Poly1305 as a MAC for ESP and AH.
- Describes the use in ESP of the AEAD AEAD_CHACHA20_POLY1305.
- The algorithms themselves are described in another document.

More about this draft

- ChaCha20 is a stream cipher, but it takes a nonce, so it is suitable for IPsec.
- Moving data from packets to internal state treats them as ***little-endian*** numbers.
- Poly1305 MAC needs a one-time key for each packet
  - We use ChaCha20 as a PRF with the replay counter as the nonce.
  - Needs access to the replay counter.

More about this draft

- Adam Langly's AEAD
  - MACs [AAD||len(AAD)||ciphertext||len(ciphertext)].
  - Unlike GCM, lengths are 64-bit little-endian and expressed in bytes, not bits.
  - Does not need access to the replay counter, because we use the same key for encryption and for generating the Poly1305 keys.

Questions for this Group

- Are people fine with these design decisions?
- Should this be a WG draft?
- Do you think we should apply for early IANA number assignment?
- Other comments

Thanks