IKEv2 Negotiation for EESP

draft-ietf-ipsecme-eesp-ikev2-01

Steffen Klassert (steffen.klassert@secunet.com)
Antony Antony (antony.antony@secunet.com)
Tobias Brunner (tobias@codelabs.ch)
Valery Smyslov (svan@elvis.ru)

IETF 124

EESP

Enhanced **E**ncapsulating **S**ecurity **P**ayload
(draft-ietf-ipsecme-eesp)

Key features:

- Versioning
- Sub SAs
- Optional 64-bit Sequence Number fully sent in packet
- Optional header fields to accommodate different needs
- etc.

Negotiation of EESP in IKEv2

Defined in [draft-ietf-ipsecme-eesp-ikev2]

What is being negotiated:

- Use of EESP
- EESP version
- EESP transforms
- Use of Sub SAs
  - Sub SAs key derivation
  - Maximum number of incoming Sub SAs
- SN properties
- Maximum crypto offset (**new!**)

What is New in -01 Version

- Added the ability for peers to indicate maximum crypto offset they are willing to accept
- Few clarifications in the text

Maximum Crypto Offset

- Each peer may optionally indicate the maximum value it can accept in the EESP `Crypt Offset` option by sending new EESP_MAX_CRYPT_OFFSET status notify
- It contains a one-byte value indicating the maximum crypto offset that the sender of the notify will accept as EESP SA receiver
  - the size of the `Crypt Offset` option in EESP packet is 6 bits, thus 1 byte is enough
- These values can be different for each peer (no negotiation!)
- If this notification is not included (or contained value 0), then the host sending this message states that it does not want to receive EESP packets with non-zero `Crypt Offset`
  - if its peer violates this, such packets MUST be dropped and EESP SA SHOULD be deleted

Thanks!

Questions?

Comments?