IKEv2 Negotiation for EESP

draft-klassert-ipsecme-eesp-ikev2-00

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

IETF 122

EESP

Enhanced **E**ncapsulating **S**ecurity **P**ayload
(draft-klassert-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-klassert-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

Use of EESP and EESP Version

- Each version of EESP is considered as a separate Security Protocol in IKEv2
  - each version of EESP is proposed in separate Proposal substructure in SA payload
    - can have its own set of mandatory/optional transforms types and transform IDs
- Currently the only defined EESP version is 0
  - A new Security Protocol EESPv0 is defined

EESPv0 Transforms

- Mandatory transforms:
  - `ENCR, SN`
    - only AEAD transforms are allowed
- Optional transforms:
  - `KE, ADDKE*, SSKDF`

Sequence Numbers in EESPv0

- SN is optional in EESP, its size in EESP packet is 64 bits
  - existing values for SN transform cannot be used
    - cannot specify the absence of SN in packet
    - cannot specify that 64-bit SN is fully transmitted
  - two new values are added for SN transform for EESPv0
    - `64-bit Sequential Numbers`
    - `None`

EESPv0 Sub SAs

- Negotiation the use of Sub SAs is performed via new `SSKDF` transform, that determines KDF for Sub SA key calculation:
    - `SSKDF_HKDF_SHA2_256`
    - `SSKDF_HKDF_SHA2_384`
    - `SSKDF_HKDF_SHA2_512`
    - `SSKDF_AES256_CMAC`
- if no KDF is negotiated, then Sub SAs are not used for the EESP SA

EESPv0 Sub SAs Max Number

- Each peer may optionally indicate the maximum number of Sub SAs it can handle as EESP SA receiver by sending new EESP_MAX_SUB_SA_ID status notify
- It contains maximum Session ID value the sender of the notify will accept as EESP SA receiver
  - Session ID in incoming EESP packets must be in the range *0..[this value]*
- These values can be different for each peer (no negotiation!)
- Value 0 in this notify means that only 1 Sub SA is allowed
- If this notification is not included, then no restriction on the number of incoming Sub SAs is imposed by the peer sending this message

Thanks!

Questions?

Comments?