OPTIMIZED_REKEY ISSUES FOUND
DRAFT-IETF-IPSECME-IKEV2-SA-TS-PAYLOADS-OPT

IPsecME, IETF 116
Yokohama, March 2023

Tobias Brunner, Paul Wouters
OPTIMIZED_REKEY and SPI

• REKEY: IKE and Child SA contains new SPI in the SA payload
• OPTIMIZED_REKEY: Both send new SPI in N(OPTIMIZED_REKEY)
• Difference between IKE and Child rekey a little harder to detect via size difference of SPI field

• Proposal 1: Leave as is and use SPI size (and improve text)
• Proposal 2: Use a new notify payload (OPT_REKEY_IKE_SPI)?
OPTIMIZED_REKEY_SUPPORTED

• Sent in IKE_AUTH

• What if there are more than one IKE_AUTH exchange

• Proposal:
  • Initiator sends it in first IKE_AUTH
  • Responder send it in the last IKE_AUTH exchange (i.e. sent it where normally the TS payloads go)
Rekeying initial Child SA

• The initial Child SA uses the KE from the IKE SA
• If Child SA negotiates PFS, it uses the IKE SA group

• OPTIMIZED_REKEY for Child SA that used PFS should:
  • Proposal 1: Use same KE as IKE SA
  • Proposal 2: Use a regular rekey before using an optimized rekey
USE_TRANSPORT, ESP_TFC_PADDING_NOT_SUPPORTED, NON_FIRST_FRAGMENTS_ALSO, etc

- Normally sent in CREATE_CHILD_SA for rekeys.
- We don’t want a changed outcome on these notifies.

- Proposal 1: omit Notifies means “keep same”, error if not.
- Proposal 2: sent Notifies, error if not same.
IPCOMP_SUPPORTED

• IPCOMP_SUPPORTED payload contains compression algorithm and the CPI.

• Algorithm could be omitted but CPI is needed.

• Proposal 1: Send IPCOMP_SUPPORTED with new CPI.
  • Reject proposals that change IPcomp algorithm

• Proposal 2: Omit IPCOMP_SUPPORTED and send a 2nd OPTIMIZED_REKEY Notify with protocol IPcomp (108) and SPI length 2 and the new CPI as SPI value.
ERROR HANDLING

• If KE payload is for a different group, or “Child SA notify change” (see previous slides), what error message to send?
  • INVALID KE
  • INVALIX SYNTAX
  • NO_PROPOSAL_CHOSEN
  • A new: INVALID_REKEY_CHANGE