GDOI GROUPKEY-PUSH Acknowledgment Message

draft-weis-gdoi-rekey-ack-03

IETF 97, Seoul, South Korea

Brian Weis (bew@cisco.com)
Umesh Mangla (umangla@juniper.net)
Nilesh Maheshwari (nileshm@juniper.net)
Thomas Karl (thomas.karl@telekom.de)

Background

- GDOI (RFC 6407) done in msec WG and uses IKEv1.
- GDOI (RFC 6407) is a group key management method by which a Group Controller/Key Server (GCKS) distributes security associations to a set of Group Member. (GM) devices.
- GDOI describes the Rekey Protocol as a GROUPKEY-PUSH message.
- GROUPKEY-PUSH message is used by GCKS to alert GMs of updates in policy of the group including keying material.
- RFC 6407 doesn’t provide for the acknowledgment of the GROUPKEY-PUSH message.

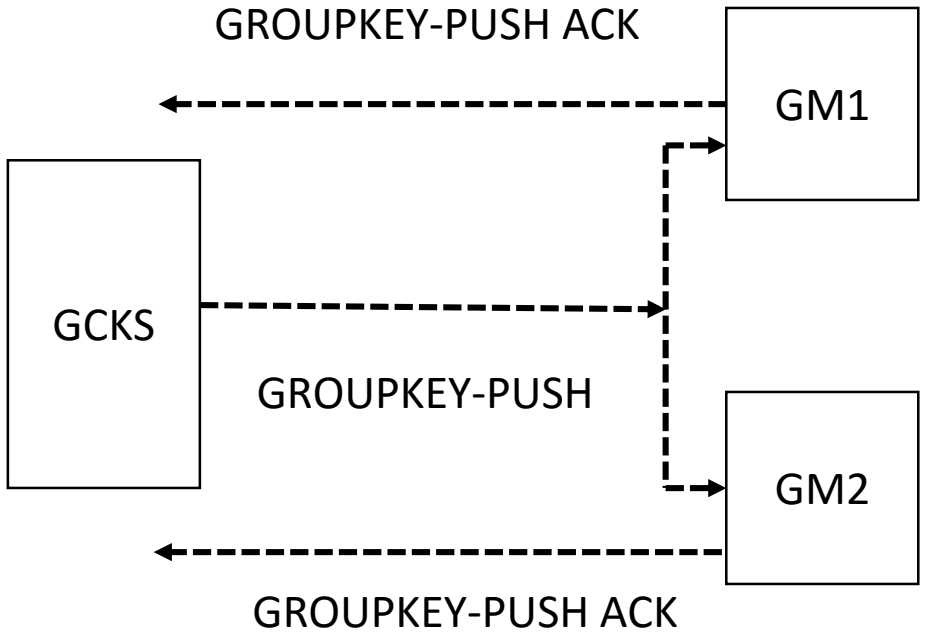
Problem Statement

- Interoperability of GCKS (Group controller key server) with GMs (Group Member) from different vendors.
- GCKS may remove the GMs from the group which cannot send acknowledgment back on receiving the rekey message.
- It is preferable for GCKS to receive the acknowledgment from GM to ensure that GM has acted on the rekey message and the policy contained in it. Our draft addresses this aspect.

Proposed Solution

- Introduce a method by which a GM returns an acknowledgment message to the GCKS.
- Initially a GCKS requests GM to acknowledge GROUPKEY-PUSH messages as part of distributed group policy.
- GCKS delivers a GROUPKEY-PUSH message, each GM that honors the GCKS request returns a GROUPKEY-PUSH Acknowledgement Message (See next slide).
- This is an optional message.

Proposed Solution Cont…



GROUPKEY-PUSH ACK Message

GM GCKS
----- -------
<---- HDR*, SEQ, [D,] SA, KD, SIG

* Protected by the Rekey SA KEK; encryption occurs after HDR
GROUPKEY-PUSH from RFC 6407

HDR, HASH, SEQ, ID ---->
GROUPKEY-PUSH Acknowledgement Message

Group Member Operations

- GM receives an SA KEK payload in a GROUPKEY-PULL exchange or GROUPKEY-PUSH message.
- Payload contains KEK_ACK_REQUESTED attribute. GM updates its group state such that it responds with acknowledgment to GROUPKEY-PUSH message.
- GROUPKEY-PUSH ACK message is also sent if GROUPKEY-PUSH message contains a Delete payload.

GCKS Operations

- GCKS policy specifies requesting a GROUPKEY-PUSH ACK message from GMs.
- GCKS includes KEK_ACK_REQUESTED attribute in the SA KEK payload.
- GCKS includes this attribute every time the SA KEK is delivered in both GROUPKEY-PULL exchanges and GROUPKEY-PUSH messages.
- When GCKS receives a GROUPKEY-PUSH ACK message, it verifies the group policy.
- GCKS validates the message and acts as per sequence number and identity of the GM.

Next Steps?

- Draft describes a deployed solution implemented by multiple vendors.
- Looking for your technical feedback on solution.
- Given that draft is augmenting GDOI, which was done in msec, is ipsecme appropriate & enthusiastic?
- Tentative plan is for AD-sponsoring like other GDOI work (e.g. draft-weis-gdoi-iec62351-9-10).