Group Key Management using IKEv2

draft-ietf-ipsecme-g-ikev2

Valery Smyslov
ELVIS-PLUS

Brian Weis
Independent

IETF 112

Securing IP Multicast

- IP multicast applications
  - Contain at least 1 sender, and N receivers
  - Take advantage of the network to route and replicate IP packets, such that the same packet reaches all N receivers
- This requires senders and receivers to share setup an IPsec SA using the same keys
  - The IPsec policy and keys are not negotiated, but instead they are distributed by a Group Controller / Key Server (GCKS) to Group Members (GMs)
  - A GM invokes a unicast Registration protocol to authenticate to the GCKS. The GCKS then authorizes the GM, and distributes IPsec policy and keys to the GM.
  - A Rekey protocol enforces a time-based key rollover strategy

Distribution of Group Keys in IEEE 802.15

- IEEE 802.15.9 specified IKEv2 as one of KMPs for IEEE 802.15.4
  - IEEE Std 802.15.9-2015 left group keys distribution out of scope
- Draft 05 version of the IEEE Std 802.15.9 standard (March 2021) specifies that G-IKEv2 is used for group key distribution
  - GSA_INBAND_REKEY over unicast SA is used
  - SPI field in GSA payload is used to specify the type of group key

Document Status

- Has been in development for several years
  - few implementations of early draft versions exist
- Has been adopted by IPSECME WG in 2019
- Version -01 (July 2020): major rewrite
- Version -02 (January 2021): minor update
- Version -03 (July 2021): minor update
- For authors the draft looks mature
  - however, more reviews are needed

Outline of -01 Changes

- Policy representation changed
  - before: IKEv1 style, mostly using attributes
  - now: IKEv2 style – using transforms, attributes are still used to represent variables
- Format of GSA and KD payloads changed
- Group keys representation changed
  - before: group keys were transferred in clear inside KD payload
  - now: all keys are encrypted inside KD payload, using either SK_d derived key or other group key
- LKH (Logical Key Hierarchy) is integrated in core G-IKEv2
  - before: dedicated attributes were used to transfer LKH keys
  - now: LKH functionality is integrated into the core G-IKEv2 protocol, GM semantics doesn’t depend on key management method

Outline of -01 Changes (cont.)

- IANA considerations are rewritten
  - now it’s more an extension to IKEv2 than a separate protocol (IKEv2 IANA registries are used)
  - many parameters have been renamed to better reflect their purpose
- A lot of clarifications
  - AUTH payload calculation for GSA_REKEY messages is described in details
  - introduced means to indicate cross-dependency of supported algorithms in SAg payload
  - using PPK in G-IKEv2 is clarified
  - using ESN is clarified (in -02)
  - failover in situations when rekey message was missed clarified (using NEXT_SPI)
  - example of using LKH is rewritten

GSA Payload

Contains policy necessary to participating in the group:

- Protocol (GIKE_REKEY, AH, ESP)
- Traffic Selector
- Transforms for algorithms and methods used in the policy
- Attributes for variables that change over time (like initial Message-ID)
- GSA format is now common for KEK (GIKE_REKEY) and TEK (AH, ESP)
  - GAP (Group Policy) shares the same format and is distinguished by zero protocol

KD Payload

Contains keying material necessary for the policy in the GSA payload:

- One or more keys are conveyed in the KD payload
- Security parameters are also conveyed in the KD payload
- Each key is individually wrapped in a new structure Wrapped Key
- Each Wrapped Key structure is encrypted using either SK_d derived key or other group key
- LKH capability is now integrated into G-IKEv2 core and is achieved by including several keys into the KD payload logically linked by encrypting next key in the tree with previous one
- Wrapped Keys may contain either group keys (common for a whole group or for subset of its members) or member keys (allows for provision keys for a member during GSA registration, needed for LKH)

IDg Payload

Contains identity of the group a GM wants to join (no changes since -00):

- has the same format as IKEv2 ID payload
- only some ID types are expected to be used
  - ID_KEY_ID MUST be supported
  - ID_IPV4_ADDR, ID_IPV6_ADDR , ID_FQDN , ID_RFC822_ADDR SHOULD be supported

Reused IKEv2 payloads

Payloads that have the same types as in IKEv2, but different semantics:

- SAg (GM Supported Transforms)
  - declares which Transforms a GM is willing to accept
  - has the same format as IKEv2 SA payload, but slightly different semantics, which allow to indicate inter-dependency of supported algorithms
- D (Delete Payload)
  - used when the GCKS may want to signal to group members to delete policy (e.g., data flows finished, change of policy)
  - semantics is slightly different from IKEv2, allowing to delete all SAs

New Notifications

- INVALID_GROUP_ID (error notify)
  - GCKS informs GM that the requested Group ID in a registration protocol is invalid
- AUTHORIZATION_FAILED (error notify)
  - GCKS informs GM that it is not authorized to join the requested Group ID
- REGISTRATION_FAILED (error notify)
  - GCKS informs GM that for some reason the GM cannot join the group
  - GM sends to GCKS to unregister from the group
- SENDER (status notify)
  - GM informs the GCKS about its intention to be a sender in the group
  - requests a number of Sender-ID values, that are used as part of a counter-mode transform nonce (RFC 6054)
- REKEY_IS_NEEDED (status notify) – added in -01
  - GCKS informs GM that it must rekey IKE SA before receiving sensitive information (used in PPK scenarios)

Reused IKEv2 Notifications

- USE_TRANSPORT_MODE
  - semantics is changed, so that Protocol and SPI fields are used to indicate which SA to create in transport mode
  - multiple instances can be sent if multiple SAs are being created

Thank you!

- Comments?
- Questions?
- Please review the document
  - WGLC?