Key Management for Pairwise Routing Protocol

draft-mahesh-karp-kmprp-00

Mahesh Jethanandani, Brian Weis, Keyur Patel

IETF 81, July 2011, Quebec City, Canada

Motivation

- Key Management limited to static configuration of Master Keys in individual Routers
- No way to automatically exchange key material related information between pairwise network devices that has routing protocol adjacencies setup
- Need for an automated exchange of key material is articulated in draft-ietf-karp-routing-tcp-analysis-00

Key Management of Pairwise Routing Protocol (KMPRP)

- Used to automatically exchange private key material related information between two network devices forming a TCP based/point-to-point routing protocol adjacency
- Uses IKEv2 like protocol exchanges, state machine and policy definitions
- Defines a new dedicated UDP port for IKEv2 exchanges to distinguish from IPsec's usage

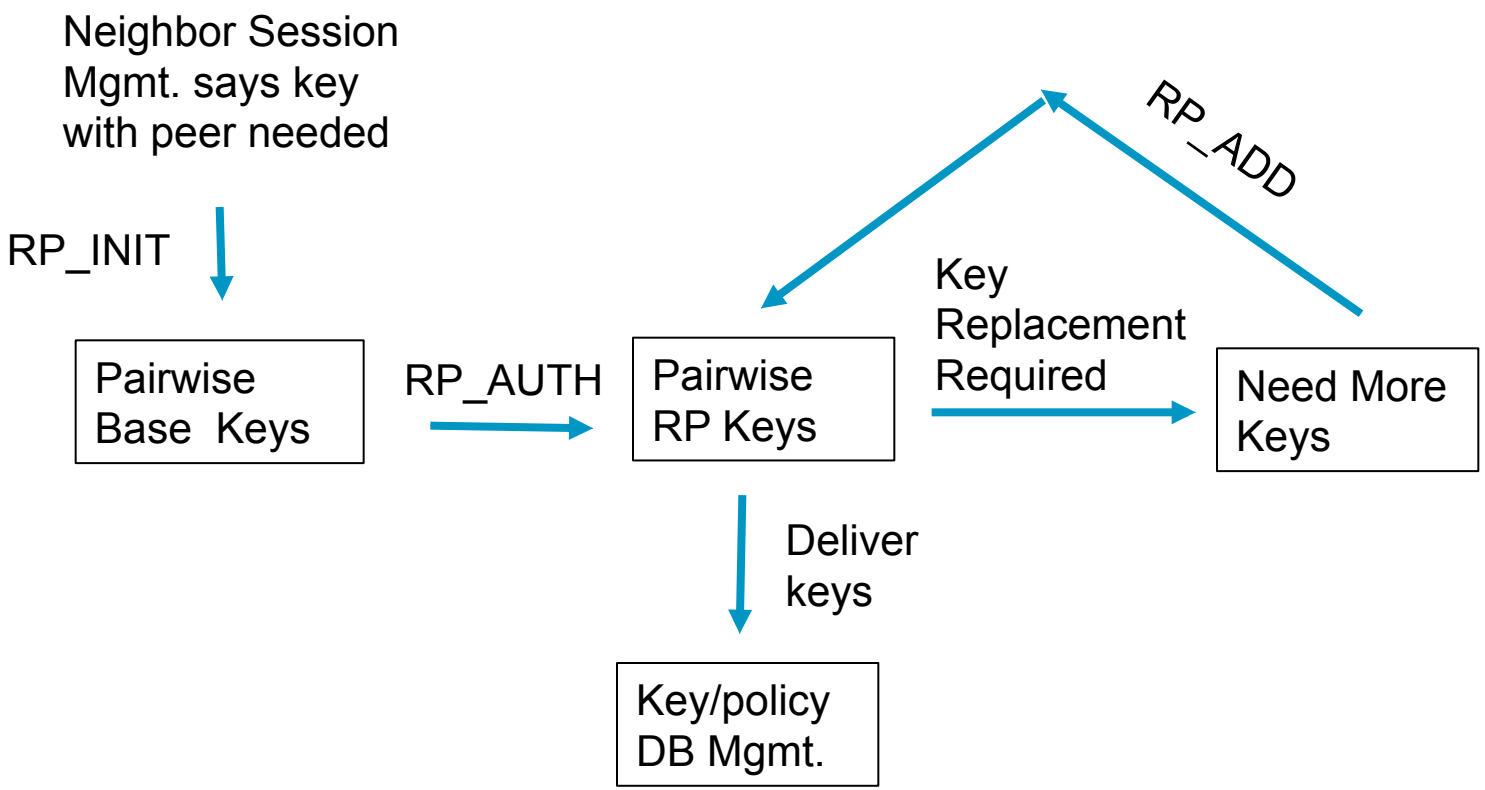
KMPRP Protocol Exchanges

- RP_INIT
  - Similar to IKE_SA_INIT exchange
  - Used to create a private channel for subsequent protocol exchanges
  - Two message exchange that allows devices to negotiate cryptographic algorithms, exchange nonces, and do a Diffie-Hellman (DH) for routing protocols
  - Two devices can communicate privately about their key related information upon successful RP_INIT exchange
- RP_AUTH
  - Similar to IKE_AUTH exchange except that the policy payload contains policy specific to routing protocol security policy
  - Initiator proposes one or more sets of security policy
  - Responder responds with one security policy it accepts
  - Upon a successful completion Initiator and Responder have negotiated and settled upon a single policy
  - A common key is derived from the Diffie-Hellman (DH) key material

KMPRP Protocol Exchanges

- RP_ADD
  - Similar to IKEv2 CREATE_CHILD exchange
  - Used to do a re-key or to negotiate key material information for new protocol
  - Routing protocol security association (SA) payloads are identical to RP_AUTH exchange
- Information message
  - Useful for deleting specific SA and/or sending status information

KMPRP State Machine



KMPRP SA Payload

- SA payload contains one or more proposals and transforms
- Proposal Substructure covers the following
  - Protocol id of protocols under negotiation
    - TCP AO
    - LDP Discovery Key
    - KMPRP
  - Routing protocol id under negotiation
    - BGP
    - LDP
    - MSDP
    - PCEP
  - Number of transforms and transform substructures

KMPRP SA Payload

- Transforms
  - Describes particular set of cryptographic policy choices
  - Used to announce multiple sets of such policies
  - TCP AO transform covers
    - SendID – TCP-AO KeyID
    - Authentication Algorithm – HMAC-SHA-1-96, AES
    - Key Derivation function (KDF) – HMAC-SHA-1-96, AES
    - Flags to indicate TCP options for TCP AO

KMPRP Operation

- Routing protocol initiates point to point KMPRP neighbor session as part of
  - Neighbor adjacency configuration changes
  - local rekey policy decision
- A local entry is created in KMPRP database (KMDB) that consists of the following
  - Security Algorithm
  - Key specific information
  - Routing protocol client
  - Routing protocol neighbor
- Upon a successful KMPRP neighbor session creation, RP_INIT and RP_AUTH exchanges are done
  - Key material information is exchanged as part of RP_AUTH exchange
- KMPRP neighbor session is disconnected post the key material information exchange

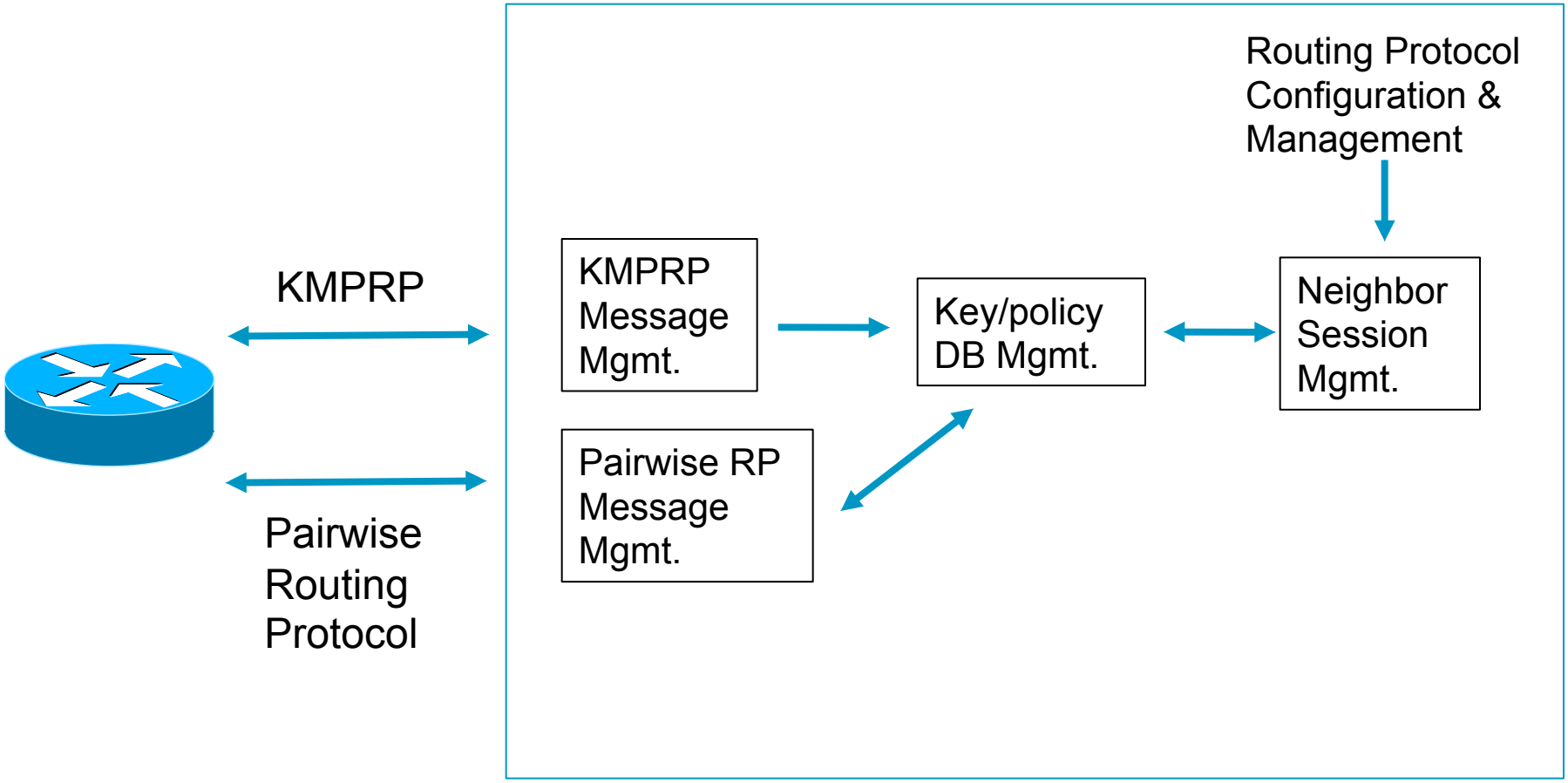
KMPRP Key Management Data Base (KMDB)

- KMDB stores
  - Entries locally created by Client Routing Protocols
  - Key related information received from KMPRP sessions
- Notifies client routing protocols about key related information updates
- Initiates sessions with KMPRP neighbors whenever a local key related information is changed

KMPRP & Routing Protocol interactions

- Routing protocols interacts with KMPRP using KMDB
- Routing protocols could end up with multiple keys with KMPRP
- Key rollover is outside the scope of this document
  - TCP AO has already defined its own key rollover mechanism
  - Implementations should store old keys for certain period of time so as to handle out-of-order packets correctly

KMPRP Operation



Questions?