Key Management for Pairwise Routing Protocol
draft-mahesh-karp-rkmp-00

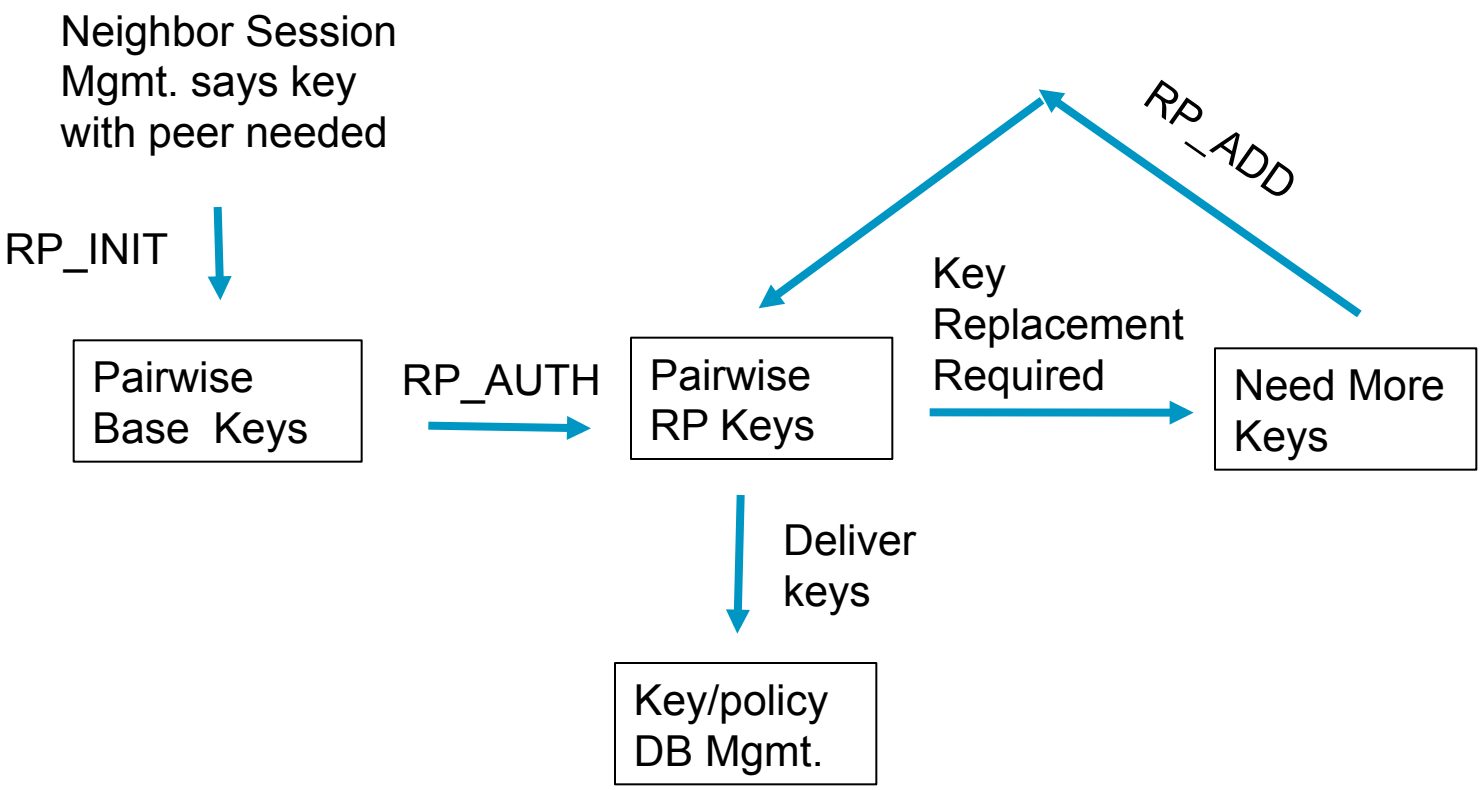
Mahesh Jethanandani, Brian Weis, Keyur Patel, Dacheng Zhang, Sam Hartman

IETF 82, Nov. 2011, Taipei, Taiwan

Introduction

- A combination of “draft-mahesh-karp-kmprp-00” and “draft-zhang-karp-rkmp-00”
- Aims to generate an automatic key management for pairwise routing protocols
  - Cooperate with RKMP to make a integrated KMP Solution for routing protocols
  - The initial exchanges will be adopted by RKMP
- Takes advantage of the work of IKEv2 as much as possible, but generalize it to support different routing protocols

RKMP State Machine



Exchanges

- RP_INIT:
  - Allows the network devices to negotiate cryptographic algorithms, exchange nonce, and do a Diffe-Hellman agreement
  - Based on IKEv2's IKE_SA_INIT exchange
- RP_AUTH:
  - Used to generate RKMP_SAs and protocol master keys
  - Based on the IKE_SA_AUTH exchange in IKEv2
  - Expected to support various routing protocols

RKMP 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

Security Association 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
    - RKMP
  - Transform substructures which describe particular sets of cryptographic policy choices. For instance, a 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

Traffic Selector Payload

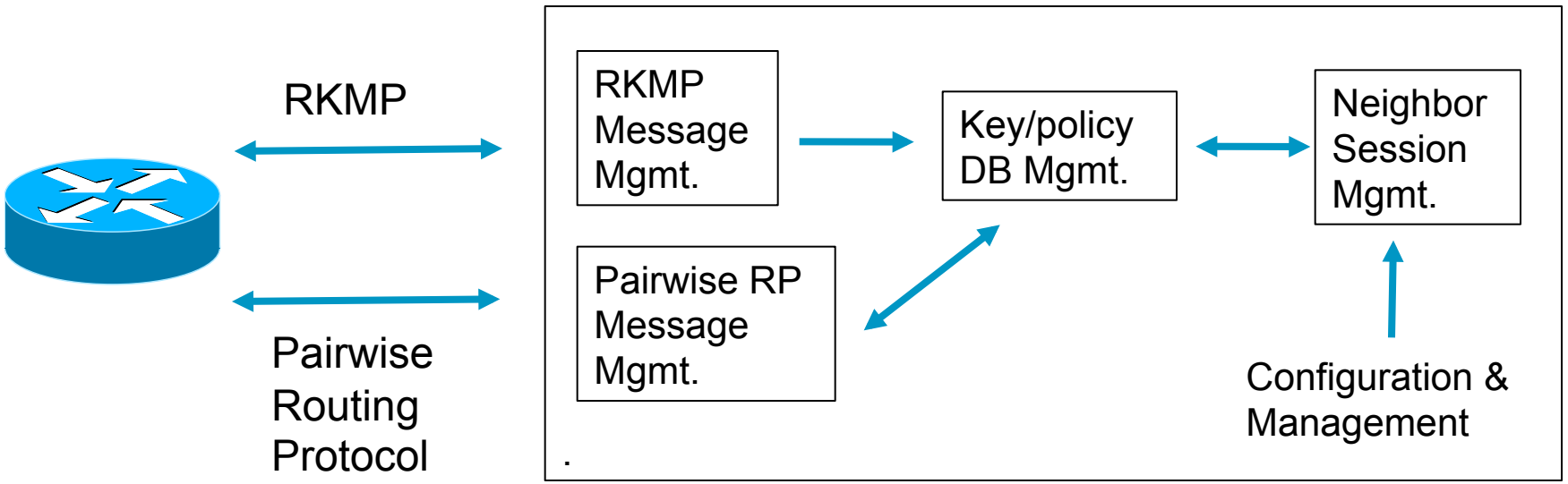
- The Traffic Selector (TS) payload definition is the same as defined in Section 3.13 of IKEv2 [RFC5996].
- A traffic selector contains the routing protocol id under negotiation

Routing (RT) Protocol	Protocol ID	Reference
BGP	1	RFC 4271
LDP	2	RFC 5036
MSDP	3	RFC 3618
PIM PORT	4	
PCEP	5	RFC 5440

Routing Protocol

RKMP Operation

- Routing protocols control KMP through Key Management Data Base (KMDB)
- Routing protocols could end up with multiple keys with RKMP



RKMP Key Management Data Base (KMDB)

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

RKMP Operation

- Routing protocol initiates point to point RKMP neighbor session as part of
  - Neighbor adjacency configuration changes
  - local rekey policy decision
- A local entry is created in RKMP database (KMDB) that consists of the following
  - Security Algorithm
  - Key specific information
  - Routing protocol client
  - Routing protocol neighbor

RKMP Operation (cont.)

- Upon a successful RKMP neighbor session creation, RP_INIT and RP_AUTH exchanges are done
  - Key material information is exchanged as part of RP_AUTH exchange
- RKMP neighbor session is disconnected post the key material information exchange

Questions?