Key Management for Pairwise Routing Protocol

draft-mahesh-karp-rkmp-01

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

IETF 83, March 2012, Paris, France

Introduction

- Aims to generate an automatic key management for pairwise routing protocols by extending IKEv2
  - –IKEv2 payload definition and exchanges are kept unchanged
  - –new security policy definitions are described to support security transforms and policy defined by routing protocols

Updates (1)

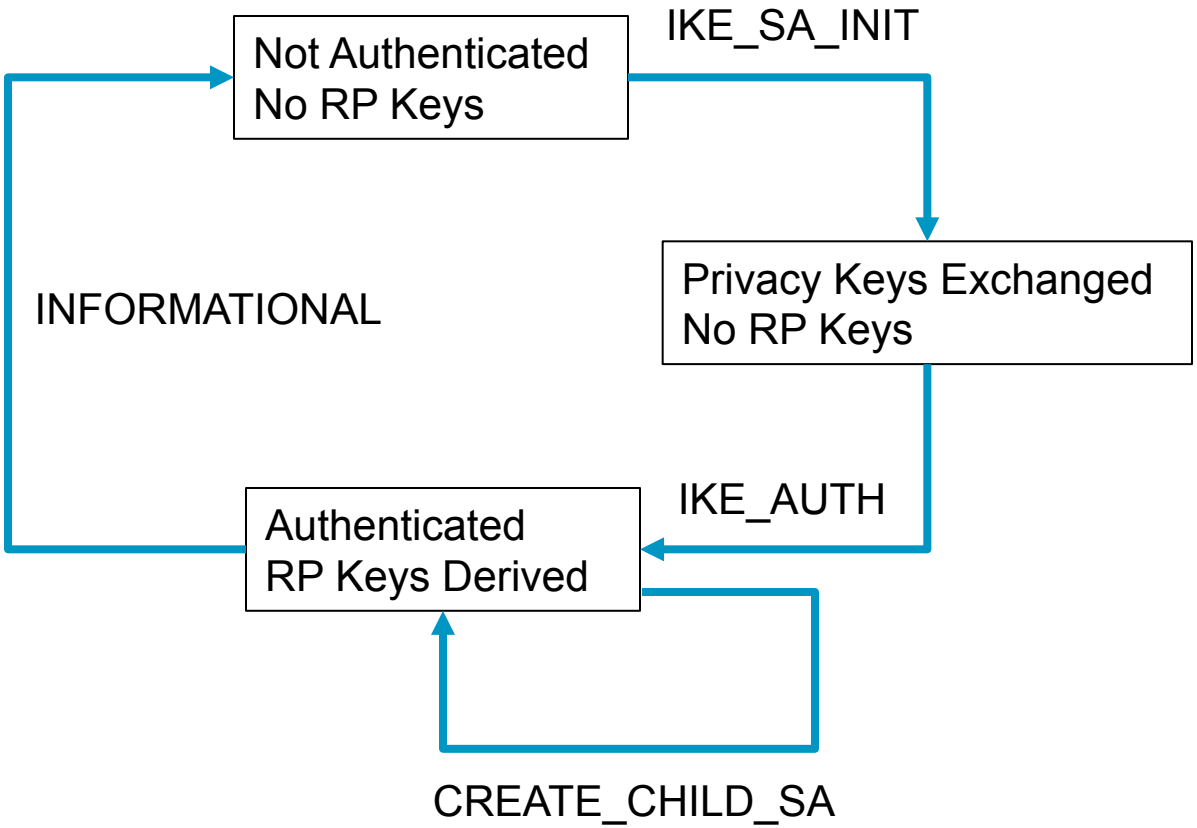
- Use the terms of IKEv2 instead of defining new terms
  - –RP_INIT → IKE_SA_INIT
  - –RP_AUTH → IKE_AUTH
  - –RP_ADD → CREATE_CHILD_SA
  - –RKMP Header → IKEv2 Header
  - –RP SA → IKEv2 SA

Updates (2)

- Key Selection, Rollover and Protocol Interaction

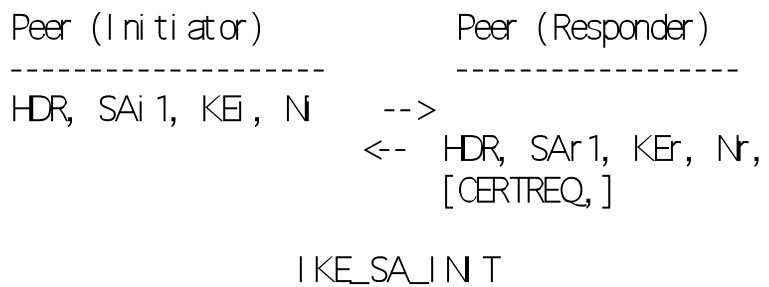
  The procedure for key selection and rollover exchange and Details of how RP interact with KMDB and deals with multiple keys during rollover has been described in Database of Long-Lived Symmetric Cryptographic Keys [I-D.ietf-karp-crypto-key-table] and is out of scope of this draft.

RKMP State Machine

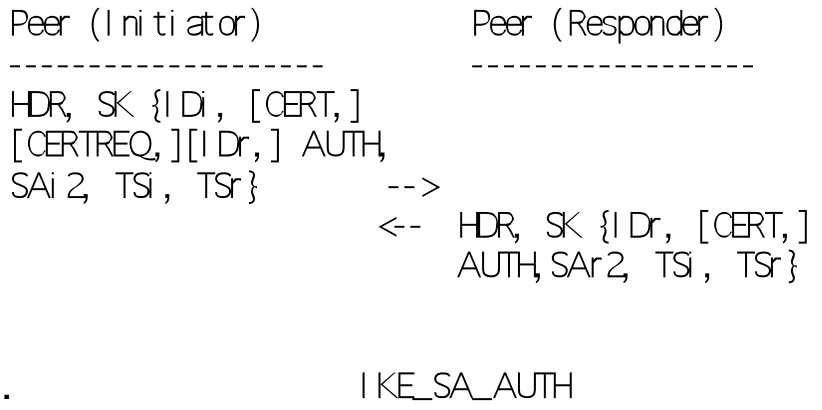


Exchanges

- IKE_SA_INIT:
  - –Allows network devices to negotiate cryptographic algorithms, exchange nonces, and do a Diffe-Hellman exchange for their routing protocols,
  - –After which, routing protocols on these network devices can communicate privately.

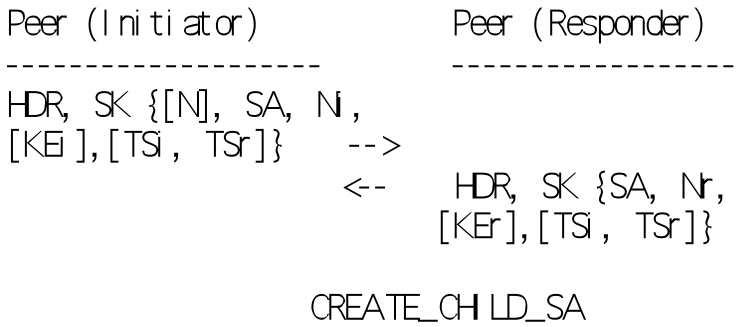


- IKE_SA_AUTH :
  - –Expected to support various routing protocols
  - –the SA payloads contain the routing protocol specific security policies rather than IPsec policies (SAi2, SAr2 defined in RFC 5996)
  - –Traffic selector payloads contains routing protocol specific traffic selectors.

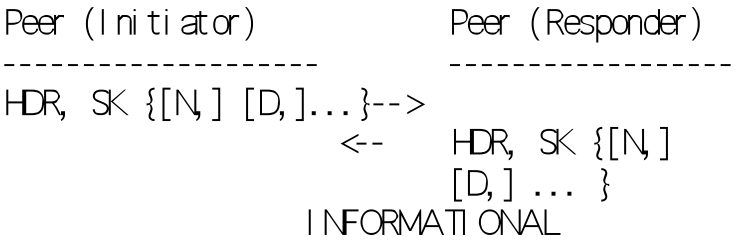


RKMP Exchanges

- CREATE_CHILD_SA
  - –Rekey an antique RP master key and establish a new equivalent one
  - –Generate needed key material for a newly executed routing protocol based on an existing SA
  - –Rekey an IKEv2 SA and establish a new equivalent IKEv2 SA.



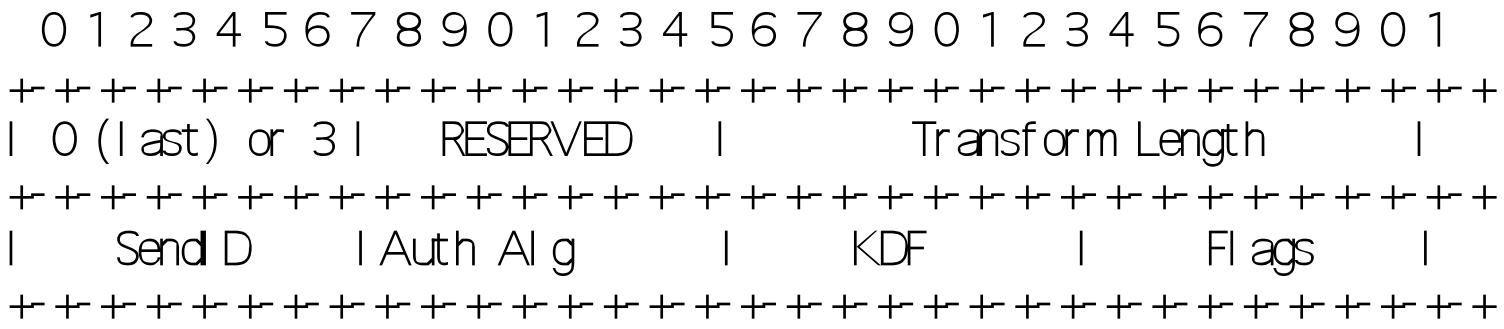
- Information message
  - – Useful for deleting specific SA and/or sending status information



Security Association Payload

- SA payload contains one or more proposals and transforms
- Proposal Substructure covers the following
  - More value of Protocol ID filed is defined for different routing protcols, e.g.,
    - TCP AO
    - LDP Discovery Key
  - Transform substructures which describe particular sets of cryptographic policy choices for different protocols, such as TCP AO

TCP-AO Transform



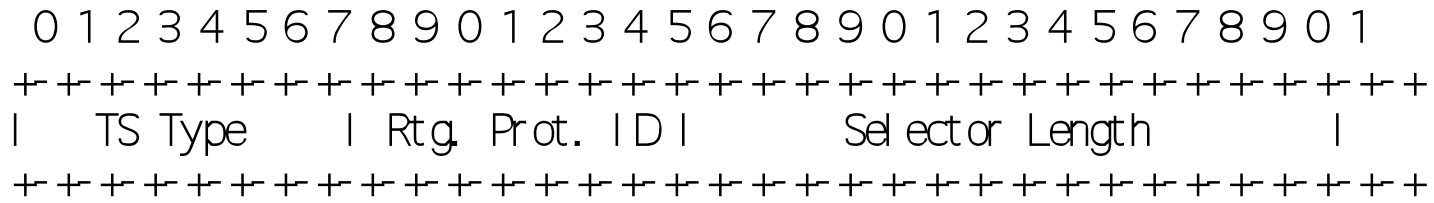
- When a TCP-AO transform is chosen, keying material for the TCP-AO master key is generated as follows,

  <TCP-AO master key> = prf+(SK_d, Ni | Nr)

  where Ni and Nr are unique to this exchange. The value SK_D is defined in RFC 5996, and refers to the value derived from SKEYSEED that is used to derive new keys

Traffic Selector Payload

- Unlike IPsec, routing protocols have well-defined flows, and there is no need to specify them to the specificity of IPsec policy. Therefore, a new type of TS payload is defined:



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

Questions?