Unicast Router Key Management Protocol (RKMP)

draft-zhang-karp-rkmp-00

Dacheng Zhang
zhangdacheng@huawei.com
Sam Hartman
hartmans@painless-security.com

Introduction

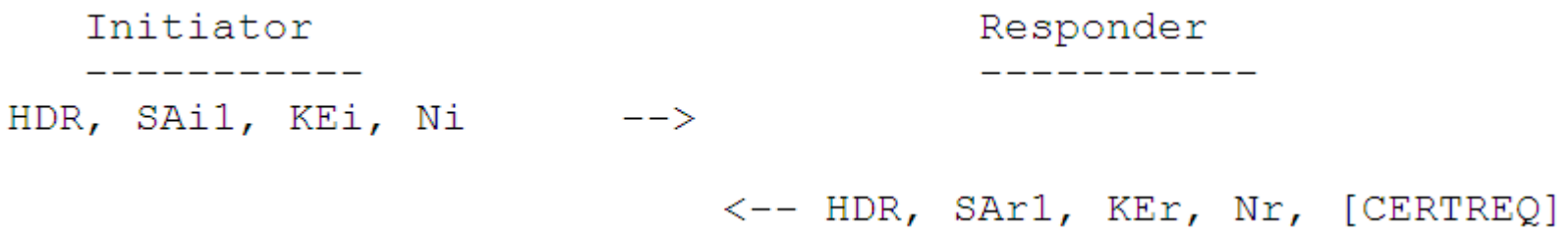
- This work is to propose a unicast KMP which can be combined with MRKMP to make a integrated KMP solution.
  - The initial exchanges will be adopted by MRKMP
- The work in IKEv2 are taken advantaged as much as possible.
  - However, the payloads only useful for IPsec are removed from the solution

Exchanges

- Initial Exchanges:
  - Used to generate RKMP_SAs and protocol master keys
  - The initial exchanges is based on IKEv2's IKE_SA_INIT and IKE_SA_AUTH exchanges, which are referred to as RKMP_SA_INIT and RKMP_SA_AUTH exchanges respectively.
- Child SA Exchange:
  - Based on the CREATE_CHILD_SA exchange in IKEv2
  - Expected to support various routing protocols

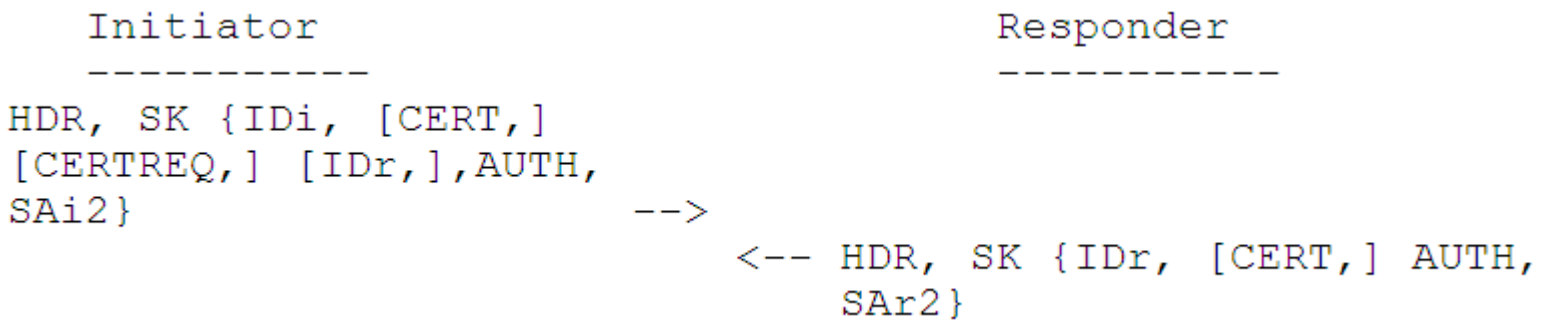
RKMP_SA_INIT

- The payloads included in the RKMP_SA_INIT exchange are identical to what have been specified in the IKE_SA_INIT exchange [RFC4306].
- During the RKMP_SA_INIT exchange, the two communicating partners need to identify the cryptographic suite they both support, exchange nonce in order to check each other's aliveness, and exchange their public keys.
- After the exchange, both partners can use the Diffie-Hellman algorithm to agree upon a shared secret from which all keys for securing subsequent messages are derived.



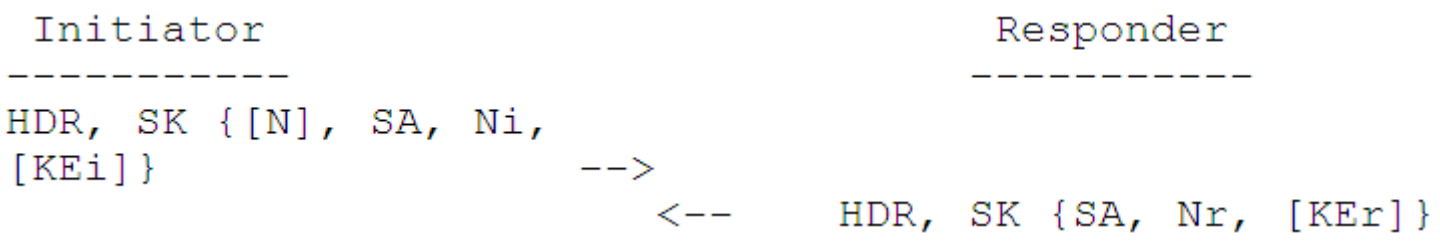
RKMP_SA_AUTH

- The RKMP_SA_AUTH exchange employs most of the payload specified in the IKE_SA_AUTH exchange.
  - The traffic selector payloads in the original IKE_SA_AUTH exchange is removed.



Child SA Exchange

- The child SA exchange takes advantage of the payloads of the CREATE_CHILD_SA exchange while removing the traffic selector payloads.
- In order to support different routing protocols more values of the fields in the Security Association payload needs to be defined.



Interface to RKMP

- **RKMP_generateSA**: This method is invoked when a routing protocol expects RKMP to generate a new routing protocol SA and store it into the key table.
- **RKMP_rekeySA**: This method can be invoked when a routing protocol intends to proactively rekey an child SA which is still in its valid period.

Interface to the Key Table

- **Keytable_getSA**: This method is called when a routing protocol intends to get key material to secure a routing message sent to a remote router.
- **Keytable_delete**: This method is called when a routing protocol intends to delete un-useful child SAs to release occupied resources.
- **Keytable_insertSA**: This method is called when RKMP have generated a new routing protocol SA and intends to store it into the key table
- **Keytable_rekeySA**: This method is called when RKMP have generated a equivalent SA and intends to use it take place of the existing one maintained in the key table.

Interface to a Routing Protocol

- **RP_revokeSA**: This method is called when RKMP deems that the RKMP security association has failed and then discards all state associated with the RKMP SA and any child SAs negotiated using that RKMP SA. After being invoked, the routing protocol will not use existing SAs to secure routing protocols messages.

Future Work

- Extend the SA payload to support various routing protocols
- Complete the interface to routing protocols
- Collect comments