Operations Model for Router Keying

draft-ietf-karp-ops-model-03

S. Hartman

D. Zhang

Update Discussion Related with Key Table (1)

- [I-D.housley-saag-crypto-key-table]->[I-D.ietf-karp-crypto-key-table]
- Remove the discussion about the limitations introduced by the key IDs in key table.
- Change the name of section 3.3 from “Protocol Limitations from the Key Table” to “Interactions with Automated Key Management”

Update Discussion Related with Key Table (2)

- Each routing protocol is responsible for defining the form of the Peer specification used by that protocol.
- Thus each routing protocol needs to define the scope of keys.
  - For group keying, the Peer specification names the group.
  - A protocol could define a Peer specification indicating the key had a link scope and also a Peer specification for scoping a key to a specific area.
  - For link-scoped keys it is generally best to define a single Peer specification indicating the key has a link scope and to use interface restrictions to restrict the key to the appropriate link.

Add Discussion about Notification Mechanism

- Notifications will play a critical role in avoiding security faults. Implementations SHOULD use appropriate mechanisms to notify operators
- Notifications can include messages to consoles, logged events, SNMP traps, or notifications within a routing protocol. One strategy is to have increasing escalations of notifications.

END