YANG Key-Chain
IETF 92, Dallas

Acee Lindem, Cisco
Yingzhen Qu, Cisco
Derek Yeung, Cisco
Helen Chen, Ericsson
Jeffrey Zhang, Juniper
Yi Yang, Cisco

Requirements

- Provide model definition for industry de facto standard key-chain
- Base model for protocol authentication import for (OSPF, ISIS, and others to follow)
- Support graceful key/algorithm rollover.
- Provide containers for key-chain entries and authentication protocols.

Model Structure

- Global List of key-chains
- Each key-chain has list of keys (reusable container)
    - Send/Accept Lifetime or Send and Accept Lifetime
        - Lifetime (reusable container) supports multiple specification options
    - Algorithm (reusable container)
    - Key

Model Extension

- Key container can be reused to define key-chains at other scoping levels.
- Algorithm list can be reused directly by applications requiring authentication/ encryption
    - Already done for OSPF and ISIS
- Key container extended in draft-chen-rtg-key-table-yang-00.txt for RFC 7210.

Key/Algorithm Graceful Roll Over

- Key-chain updated to include new key whose accept-lifetime overlaps the old key’s accept-lifetime (Rollover period).
  - New Key’s send lifetime doesn’t start until all devices in domain of the key-chain are updated.
- Assure that all network devices are updated and clocks are “roughly” synchronized (e.g., using NTP).

Key/Algorithm Graceful Roll Over (Continued)

- When the send lifetime is valid, all the network devices should start using the new key (always transmit with the key with the most recent send lifetime start).
- Old key can be removed from the key-chain. However, you may wait until the next key rollover – 2 keys in chain:
  - Current and Previous (Steady State)
  - Current and Future (Rollover Period)

Summary

- Model represents reusable authentication/ encryption policy – attach anywhere.
- Immediate use is for M2M programming of keys for routing protocol models.
- After rollout, no reason not to automate key rollover.
- Base model can be extended through augmentation.
- Requires swift and decisive WG adoption!!!