Supporting Multicast Routing Protocols Using Keytable

Tim Polk
Russ Housley
Background

- Concept was separation of routing protocol from management of long term keys
- Documented in two personal drafts
  - draft-housley-saag-crypto-key-table
    - Concrete definition of a conceptual database
  - draft-polk-saag-rtg-auth-keytable
    - Informational, applying the database of long-lived cryptographic keys to routing protocols
    - Included unicast “worked example” for TCP-AO
- Applicability to multicast routing unclear
Target: IS-IS

• Authors decided to develop a worked example for IS-IS as a stress test since this seemed the most complex
  – Network Entity Title instead of IP address in keytable definition
  – New worked example text in informational draft

• Two new drafts believed to demonstrate applicability to multicast (and resolve all known comments)
  – draft-housley-saag-crypto-key-table-04
  – draft-polk-saag-rtg-auth-keytable-05
Overview of IS-IS Example (0)

• Goals authentication and replay protection
  – Relies on RFC 5310 for authentication TLV
  – Relies on native IS-IS sequence numbers for replay protection in link state PDUs
  – Assumes existence of a “timestamp” TLV to add replay detection for IS-IS hellos
Overview of IS-IS Example (1)

• Required key material mimics password-based configuration
  – a pairwise key for each point-to-point link to protect hello messages;
  – a multicast key for each broadcast LAN, for each Level, to protect hello messages;
  – a multicast key for LSP and sequence number packets for each Level 1 area; and
  – a multicast key for LSP and sequence number packets for the Level 2 domain.
Overview of IS-IS Example (2)

• Each IS-IS router maintains separate keys for the IIHs on each network interface
  – Need two keys if network interface supports neighbors for the Level 1 Area and the Level 2 domain
  – If replay protection is needed, include local timestamp (sufficient to be locally increasing)

• Receiver verifies MAC, interface, and timestamp
  – Each IS-IS router needs to maintain one new state value for each neighbor (last time value)
    • Once replay protection is on, need to maintain last received timestamp for that neighbor
    • If timestamp is expected, discard IIHs that omit timestamp or include “old” timestamp value
Overview of IS-IS Example (3)

• Maintain additional key or keys to protect LSPs flooded through the Area and/or the Level 2 domain
  – Again, requires two keys if router participates in both Levels (1/2) of IS-IS

• The same procedures apply to sequence number packets
Non-features of IS-IS Example

• No key diversification needed
  – No connection-oriented communications, so typical key diversification info not available
  – Sequence numbers and timestamps provide replay protection

• No automatic rekey
  – As a practical matter, sequence number space should never be exhausted.
Changes to crypto-key-table

• IS-IS specific changes since Maastricht:
  – Added an Interface field to disambiguate peers
  – Added text regarding multicast key selection
    • Original text was more consistent with unicast

• Several additional changes to address comments from Ran Atkinson
Conclusion

• Keytable construct *can* be applied to multicast routing protocols

• Please consider whether this pair of drafts are appropriate for adoption by the karp wg.