KARP IS-IS security gap analysis

draft-chunduri-karp-is-is-gap-analysis-00

Uma Chunduri, Albert Tian, Wenhu Lu

Ericsson Inc.

IETF 82, Taipei, Taiwan

November 13-18, 2011

KARP IS-IS security gap analysis

This draft summarizes

- the current state of cryptographic key usage in IS-IS protocol
- several previous efforts to analyze IS-IS security
  - base IS-IS specification [RFC1195]
  - [RFC5304], [RFC5310] and [RFC6039]

KARP IS-IS security gap analysis (cont.)

Analysis per ietf-karp-design-guide & ietf-karp-threats-reqs

- Current State of key usage
- Threat analysis
- Per KARP Design Guide: Requirements for PH-1 (manual keying)
- Per KARP Design Guide: Requirements for PH-2 (Auto Keying)

KARP IS-IS security gap analysis (cont.)

IS-IS Security Aspects: Current State

- Separate keys for SN Dependent (IIH) and SN independent (LSPs & SNPs)
- Mostly MD5 (RFC 5304) based systems. SHA family added in RFC 5310.
- No coordinated key change mechanism across the group.

KARP IS-IS security gap analysis (cont.)

Threats in scope

Replay Attacks (intra/inter session)

- IIH replay in broadcast network to bounce ADJ
- Replayed LSP from cold booted router
- Replayed SNPs

Spoofing Attacks

- Keys shared across L1 area/ L2 domain
- Compromised keys can disrupt routing

DoS Attacks

- overwhelming load of spoofed but integrity protected protocol packets to increase the work load on the router

KARP IS-IS security gap analysis (cont.)

For manual key systems

- basic constructs for sequence/extended sequence number should be present in all IS-IS messages
- Simplified Mechanism to change the keys with out impacting the protocol operation
  - Should not affect ADJ, protocol operation (delayed flooding etc..)
  - Should not incur packet loss
  - Incrementally deployable with KMP

For KMP

- All messages in L1 area or L2 domain should use the group keys.
- Key agility with out impacting the protocol operation for re-key
- Use of crypto tables for key management should be defined for IS-IS

Sequence Number Construct for IS-IS protocol messages:

IS-IS Extended Sequence number TLV

draft-chunduri-isis-extended-sequence-no-tlv-00

- Solution is similar as done for other IGPs but applied for IS-IS protocol
- To be presented in IS-IS WG first as asked by KARP chairs
  - We welcome feedback

Questions & Comments?

Thank You!