KARP IS-IS security gap analysis

draft-chunduri-karp-is-is-gap-analysis-01

Uma Chunduri, Albert Tian, Wenhu Lu

Ericsson Inc.

IETF 83, Paris, France

March 26-30, 2012

KARP IS-IS security gap analysis

Presented at IETF-81, Taipei

Quick Recap:

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] etc..

Analysis per RFC 6518 (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)

Specific Questions from KARP (IETF-82) #1

- On LSP remaining lifetime not covered by AUTH and impact of zero remaining life time (also specified in RFC 6039)
  - No threat as implementations are supposed to accept purges
    - only LSP header and AUTH TLV
    - Full LSP packet not accepted

Specific Questions from KARP (IETF-82) #2

- Threat with CSNP (Complete Sequence number packet) itself
  - Attacks related to DoS, by replaying old CSNPs in broadcast networks
    - Processing burden on receiver
    - May cause PSNPs in the network
- Replayed LSP packet with close to Max SEQ no
  - Can cause shutdown for MaxAge+ZeroAgeLifetime (ISO default value: 20+ min) to make old LSPs to age out
    - But a node may never generate Max SEQ for an adversary to capture the same and replay (compromised keys are out of scope)

Next Steps

- further feedback and comments
- and request WG adoption

Questions & Comments?

Thank You!