Analysis of LMP Security According to KARP Design Guide

Mahesh Jethanandani

Agenda

- Disclaimer
- What
- Why
- Issues
- Recommendations

Disclaimer

- Not a LMP expert
- Volunteered
- Committed to a “Ask All, Tell All” policy
  - Ask the experts
  - Tell the WG

What?

- LMP used to manage TE links
- Used for:
  - Control channel connectivity
  - Verify the physical connectivity of data links
  - Correlate link property information
  - Suppress downstream alarms
  - Localize link failures for protection/restoration purposes

... all this in multiple kinds of networks

Why?

- RFC 6862 (KARP Threats requirement) outlines 22 threats that all protocols should consider.
- LMP could be vulnerable to
  - Spoofing of control packets
  - Modification of control packets
  - Replay of control packets
  - Brute-Force Attack against key(s)

Existing Authentication Mechanisms

- [RFC4204] recommends use of IPsec.
- No requirement that headers and payload be encrypted.
- No requirement for Endpoint identity to be protected.

Transport Level

- LMP uses TCP for Test messages, otherwise it uses UDP
- The UDP message has no authentication mechanism defined

Spoofing Attack

- LMP forms multiple adjacencies
- Physical links are single hop away
  - Attacks are difficult
- Virtual links could be multiple hops away
  - Spoofed adjacencies
  - Spoofing link connectivity

DoS Attacks

- Transport Layer (over Virtual Links)
  - Spoofing, Falsification & Interference attacks

Replay Attack

- MESSAGE_ID/MESSAGE_ID_ACK included in LMP
- Monotonically increasing
- 32-bit field can wrap
- Re-initialized after cold boot
- This is even true when IPsec is used for integrity protection, because only IPsec manual keys are used.

Recommendations

- Authentication & Key Distribution
  - Use IKEv2 to negotiate SA
  - Use key table to store keys
- Message Authentication mechanism
  - IPsec for both UDP and TCP packets, or
  - TCP-AO for TCP and a new authentication tag for UDP

Recommendations

- Replay when using manual keys
  - Increase the Message_Id number space to 64 bits with 32 bits in stable memory

Next Step

- “Ask All, Tell All”
- Provide an update

Questions?