Analysis of LMP Security According to KARP Design Guide

Mahesh Jethanandani

Agenda

- What
- Why
- Recommendations

Last presented in IETF 87 in KARP WG

Disclaimer

- I am not a LMP expert
- This is an analysis according to KARP design guide

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

LMP Procedure

- Core Procedures
  - Control Channel Management
  - Link Property Correlation
- Additional Procedures
  - Link Connectivity Verification
  - Fault Management

Why?

- [RFC 6862] outlines 22 threats that all protocols should consider.

- LMP is vulnerable to
  - Spoofing of control packets
  - Modification of control packets
  - Replay of control packets
  - Breaking of the key

- LMP uses UDP
  - No authentication mechanism

Security Requirements for LMP

- Provide
  - Authentication
  - Integrity
  - Replay protection
- Confidentiality is not required
- Protection of LMP end-point is not a requirement
- Key management including automatic key rollover
- Authentication should be cryptographically sound
- Algorithm should be agile

Integrity and Authentication

- RFC 4204 recommends IPSec
  - Headers and payload need not be encrypted
  - Manual keying mode should be supported
    - No replay protection
    - No automatic re-keying
    - Only for diagnostic purposes

Issues with Inter-Session

- MESSAGE_IDs are re-initialized
  - Cold Reboot: after each reboot, the MESSAGE_IDs will be re-initialized
  - MESSAGE_ID is a 32-bit monotonically increasing number. Will rollover.

Recommendations

- Replay protection
- IPSec
- UDP authentication

Replay Protection

- MESSAGE_ID maintained in stable memory
- Local or Network clock part of MESSAGE_ID
- Increase MESSAGE_ID from 32 to 64 bit

IPSec?

- No need for encryption
- Difficult to avoid LMP traffic escaping the IPSec channel
- More light weight
  - Use IKE extensions to achieve SA
  - Use IKE for key management
  - Shameless plug for my other draft (**draft-mahesh-karp-rkmp)**

UDP Authentication

- **How to authenticate UDP payload?**
- **LDP uses a TLV to carry auth payload.**

Questions?