Analysis of BGP, LDP and MSDP Security According to KARP Design Guide

- draft-mahesh-bgp-ldp-msdp-analysis

Mahesh Jethanandani, Keyur Patel, Lianshu Zheng
IETF 80, KARP WG, Prague
Purpose

- April Fool?
- Evaluate protocols
  - Current state
  - Desired state
  - Gap analysis
  - Suggest next steps
Current state

- Evaluate protocols
  - Underlying transport
  - Security mechanisms
  - Protection features
Current State

- Transport protocol
  - ACL
  - TCP LISTEN
  - GTSM
  - TCP Robustness
  - TCP MD5
  - TCP–AO
Security mechanisms

- Key management
  - IKE and IPSec
- Encrypt protocol data
  - Is it required?
Current State (cont.)

- Protection mechanisms
  - LDP
    - Spoofing attacks
    - Discovery attacks using UDP
Optimal State

- As defined by KARP Design Guide
- Withstand transport level attacks
- Comprehensive KMP
  - No administration
  - Unique, pair wise
  - SA cover when exchanging keys
  - Keep track of the lifetime of the keys
  - Change keys
    - Periodically
    - When compromised
- Security mechanisms in the protocol
  - Authenticate
  - Validate
Gap Analysis

- Transport layer
  - TCP attacks
  - UDP
  - Connectionless reset

- Key Management
  - Lack comprehensive KMP
  - Drafts on
    - Negotiations in key management
    - LDP Hello Crypto Authentication
What next?

- Manual key management
- Automated key management
  - Distribution
  - Rollover
How to proceed...

- Update draft based on comments received
- Review the draft
- Adoption into WG?