Update to Analysis of BFD Security According to KARP Design Guide

Manav Bhatia
Dacheng Zhang
Mahesh Jethanandani

Agenda

- Why
- Current authentication algorithms
- Recommended authentication algorithms
- Impact
- Questions

Why?

- BFD used for liveliness check by
  - Routing Protocols
    - IS-IS
    - OSPFv2
    - RIPv2
  - ~~Data path~~
    - ~~MPLS(-TP)~~

Why (cont.)?

- BFD used for liveliness check by
  - Routing Protocols
    - 3 x 30 sec
    - Something shorter
  - Across AS boundaries
    - eBGP

Existing Authentication Mechanisms

- [RFC5880] describes five authentication mechanisms

Authentication Mechanisms	Features	Security Strength
Simple Password	Password transported in plain text	weak
Keyed MD5	**sequence member required to increase occasionally**	Subject to both intra and inter -session replay attacks
Keyed SHA-1	Same with Keyed MD5	Same with Keyed MD5
Meticulous Keyed MD5	**sequence member required to increase monotonically**	Subject to inter-session replay attacks
Meticulous Keyed SHA-1	Same with Meticulous Keyed MD5	Same with Meticulous Keyed MD5

Recommended Authentication Algorithms

- SHA-2
  - SHA-256
  - SHA-384
  - SHA-512
- HMAC
  - FIPS-198

Impact of Authentication Requirement

- CPU 700 MHz – Dual Core MIPS
- Meticulous algorithm
- No hardware support for authentication
- Entirely in software

Impact of Authentication Requirement (cont.)

- Time interval 10 ms
  - 30 ms detection
  - No authentication
    - 5-10 sessions (tx + rx)
  - With authentication in software
    - 1-2 sessions (tx + rx)
- Time interval of 1 sec.
  - 3 s detection
  - No authentication
    - 100-200 sessions (tx + rx)
  - With authentication
    - 20-25 sessions (tx + rx)

What next?

- Use non-Meticulous algorithms
- Hardware support for newer algorithms

Questions?