Analysis of BFD Security According to KARP Design Guide draft-ietf-karp-bfd-analysis-01

Manav Bhatia
Dacheng Zhang
Mahesh Jethanandani

Agenda

- Why
- KARP Analysis
- Existing algorithms
- Recommended algorithms
- Impact
- Conclusions
- Questions

Last presented at IETF 87 (Berlin)

Why?

- BFD used for liveliness check
  - IP BFD
    - Next hop liveliness check
    - IS-IS, OSPFv2, RIPv2
  - ~~LSP BFD~~
    - ~~MPLS(-TP)~~
    - ~~End-to-end tunnel check~~

Why (cont.)?

- BFD used for liveliness check
  - In lieu of routing protocols “hellos”
    - 3 x 30 sec
    - Something shorter
  - Across AS boundaries
    - eBGP

KARP Analysis of BFD

- KARP threat analysis [RFC 6862]
  - Replay Protection
    - 32 bit sequence number
    - Incremented every 3.3 ms in Meticulous mode
    - 24 weeks
  - Weak authentication algorithms
    - MD5 or SHA-1 based
  - DoS attacks
    - Authentication packet send at a short interval

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 as Keyed MD5	Same as Keyed MD5
Meticulous Keyed MD5	**sequence member required to increase monotonically**	Subject to inter-session replay attacks
Meticulous Keyed SHA-1	Same as Meticulous Keyed MD5	Same as Meticulous Keyed MD5

Recommended Authentication Algorithms

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

Impact of Authentication Requirement

- BFD session in software
- BFD session is offloaded (hardware assist)
- BFD session is implemented in hardware

Impact of Authentication BFD in software

- CPU 500 MHz – Dual Core Cavium
- Meticulous algorithm
- No hardware support for authentication
- Entirely in software
- SHA-256 and HMAC

Impact of Authentication BFD in software (cont.)

- Time interval 10 ms
  - 30 ms detection
  - No authentication
    - 16 sessions (tx + rx)
  - With authentication in software
    - 2 sessions (tx + rx) (prediction)

- Time interval of 1 s.
  - 3 s detection
  - No authentication
    - 1K sessions (tx + rx)
  - With authentication
    - 125 sessions (tx + rx) (prediction)

Impact of Authentication BFD with hw assist

- Meticulous algorithm
- SHA-2 and HMAC
- No hardware support for authentication
- Hardware does tx and rx
- Packet constructed in software
- FSM in software

Impact of Authentication BFD offloaded to hardware (cont.)

- Time interval 3.3 ms
  - 10 ms detection
  - No authentication
    - 2K sessions (tx + rx)
  - With authentication in software
    - 1 sessions (tx + rx) (prediction)

- Time interval of 10ms.
  - 30 ms detection
  - No authentication
    - 8K sessions (tx + rx)
  - With authentication
    - 2 sessions (tx + rx) (prediction)

Impact of Authentication BFD implemented in hw

- Meticulous algorithm
- SHA-1
- "Hardware support" for authentication
- Hardware manages entire session in hardware
  - Including FSM

Impact of Authentication BFD implemented in hw (cont.)

- Time interval 3.3 ms
  - 10 ms detection
  - No authentication
    - 128 sessions (tx + rx)
  - With authentication in software
    - 16 sessions (tx + rx)
- Time interval of 10ms.
  - 30 ms detection
  - No authentication
    - 800 sessions (tx + rx)
  - With authentication
    - 100 sessions (tx + rx)
- GMAC

Conclusions

- Carefully evaluate why and where
- Be willing to pay for it
  - In performance
  - By adding hardware auth support

Questions?