Analysis of BFD Security According to KARP Design Guide

draft-bhatia-zhang-karp-bfd-analysis-03

Manav Bhatia
Dacheng Zhang
Mahesh Jethanandani

Why?

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

What are the threats?

- [I-D.ietf-karp-threats-reqs] outlines 22 threats that all protocols should consider.
- BFD is vulnerable to
  - Replay Protection:
  - Lack of Strong Algorithms: SHA-2 is not supported
  - DoS Attacks: When malicious packets are sent at a millisecond interval, with the authentication bit set, it can cause a DoS attack.

Existing Authentication Mechanisms

- [RFC5880] describes five authentication mechanisms for securing BFD control

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

Issues with Inter-Session

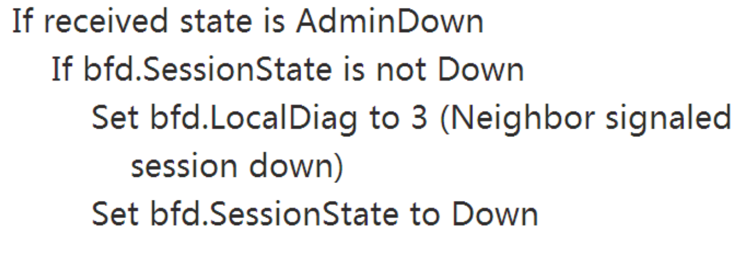
- Sequence number are re-initialized
  - Cold Reboot: after each reboot, the sequence number will be re-initialized
  - 32-bit sequence number: If sequence number is increased every 3.3 ms, it will roll over in 24 weeks
- Discriminators are not random
  - Routers pick the same discriminator after reboot

Additionally

- Limited key updating functionality
  - No smooth key rollover
- No protection of echo mode

Impacts of BFD Replays

- Force victims to change state
  - Replayed packet with the AdminDown state will force the victim set its state to Down



```
If received state is AdminDown
    If bfd.SessionState is not Down
        Set bfd.LocalDiag to 3 (Neighbor signaled
            session down)
        Set bfd.SessionState to Down
```

  - Security issues in the BFD echo mode directly affect the BFD protocol and session states, and hence the network stability.

Impact of New Authentication Requirements

- Time interval between BFD tx/rx in milliseconds
- Hardware support for authentication is not common
- Performing authentication in software impacts number of sessions that can be supported
- This is specially true for Meticulous algorithms

Recommendations

- At the re-initialization of the sequence number, a router can:
  - Change key: A Key ID is provided to the key used to hash the packet.
  - Change discriminator
- Increase the sequence number space to 64 bits
  - Wrap around in 2 million years
- Only accept sequence number in the 3 * timeout period
- Use random numbers in echo mode
- Use hardware assist in authentication

Next Step

- WG item?

Questions?