Analysis of Bidirectional Forwarding Detection (BFD) Security According to KARP Design Guide

draft-bhatia-zhang-karp-bfd-analysis-01

Manav. Bhatia
manav.bhatia@alcatel-lucent.com
Dacheng Zhang
zhangdacheng@huawei.com

Requirements to Meet

- There are several requirements described in section 3 of [I-D.ietf-karp-threats-reqs] that BFD does not currently meet:
  - Replay Protection: No inter-session replay attack is provided
  - 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 packets:

Authentication Mechanisms	Features	Security Strength
Simple Password	Password transported in plain text	weak
Keyed MD5	sequence member is only required to increase occasionally	Subject to both inner and inter -session replay attacks
Keyed SHA-1	Same with Keyed MD5	Same with Keyed MD5
Meticulous Keyed MD5	sequence member is 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 of Inter-Session Replay Attacks

- In certain cases, the sequence number will be re-initialized
  - 32-bit sequence number: If a sequence number is increased by one every millisecond, then it will reach its maximum value in less than 8 weeks
  - Cold Reboot: after each reboot, the sequence number will be re-initialized

Candidate Solutions in Tolerating Inter-Session Replay Attacks

- 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. However, no mechanism is described to provide a smooth key rollover when a BFD route moves from one key to the other.
  - Change discriminator: In existing BFD de-multiplexing mechanisms, the discriminators used in a new BFD session may be predictable. For instance, in some deployment scenarios, the discriminators of BFD routers may be decided by the destination and source addresses.

Impacts of BFD Replays

- A successful replay attack may force victims to change their state so as to cause DoS attacks.
  - For instance, according to [RFC5880], a 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
```

  - Any security issues in the BFD echo mode will directly affect the BFD protocol and session states, and hence the network stability.
    - it is important that the echo packets contain random material that is also checked upon reception.

Any Questions?