BFD: Sequence number secure encoding enhancement

Mahesh Jethanandani, Sonal Agarwal, Ashesh Mishra, Ankur Saxena,
Alan Dekok

Agenda

- Reasons for the enhancement
- Theory of operations
- Conclusion

Reasons for the enhancement

Problem:

- Sequence number’s increase monotonically.
- Predictable and vulnerable to attacks.

Solution

Solution and high level algorithm:

- Use non monotonically increasing sequence numbers.
- Hash the monotonically increasing sequence number.
- Insert hashed packet in sequence number field.

Theory of operations

- Provision the hash algorithm on the sender and receiver.
- Provision a shared key on the sender and receiver.
- Sender encodes sequence number.
- The receiver decodes the computed hash value.
- The expected sequence number should match decoded value.
- If not, it is not a legitimate packet.

Sequence number encoding

Old format of encoding sequence number (s) with values of 1, 2, 3…..

1	**2**	**3**	**4**	**5**

New format of encoding sequence number (s) with values of 1, 2, 3.... is hash(s) + key

9001	**9050**	**9070**	**9090**	**1010**

Conclusion

- Hash causes minimal performance impact.
- Increases security with or without authentication.