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.....

<p>| | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
</tbody>
</table>

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

<p>| | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>9001</td>
<td>9050</td>
<td>9070</td>
<td>9090</td>
<td>1010</td>
</tr>
</tbody>
</table>
Conclusion

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