Network Working Group
Internet-Draft
Updates: 5880 (if approved)
Intended status: Standards Track
Expires: January 14, 2021

M. Jethanandani
Kloud Services
A. Mishra
SES Networks
A. Saxena
Ciena Corporation
M. Bhatia
Nokia

July 13, 2020

Optimizing BFD Authentication
draft-ietf-bfd-optimizing-authentication-10

Abstract

This document describes an optimization to BFD Authentication as described in Section 6.7 of BFD RFC 5880. This document updates RFC 5880.

Table of Contents

1. Introduction

Authenticating every BFD [RFC5880] packet with a Simple Password, or with a MD5 Message-Digest Algorithm [RFC1321] , or Secure Hash Algorithm (SHA-1) algorithms is a computationally intensive process. This makes it difficult, if not impossible to authenticate every packet - particularly at faster rates. Also, the recent escalating series of attacks on MD5 and SHA-1 described in Finding Collisions in the Full SHA-1 [SHA-1-attack1] and New Collision Search for SHA-1 [SHA-1-attack2] raise concerns about their remaining useful lifetime as outlined in Updated Security Considerations for the MD5 Message-Digest and the HMAC-MD5 Algorithm [RFC6151] and Security Considerations for the SHA-0 and SHA-1 Message-Digest Algorithm [RFC6194]. If replaced by stronger algorithms, the computational overhead, will make the task of authenticating every packet even more difficult to achieve.

This document proposes that only BFD packets that signal a state change, a demand mode change (to D bit) or a poll sequence change (P or F bit change) in a BFD packet be categorized as a significant change. This document also proposes that all BFD control packets which signal a significant change MUST be authenticated if the session's bfd.AuthType is non-zero. Other BFD Control packets MAY be transmitted and received without the A bit set.

Most packets that are transmitted and received have no state change associated with them. Limiting authentication to packets that affect a BFD session state allows more sessions to be supported with this optimized method of authentication. Moreover, most BFD packets that

signal a significant change are generally transmitted at a slower interval of 1s, leaving enough time to compute the hash.

To detect a Man In the Middle (MITM) attack, it is also proposed that a BFD control packet without a significant change be authenticated occasionally. The interval of this non-state change frame can be configured depending on the detect multiplier and the capability of the system. As an example, this could be equal to the detect multiplier number of packets.

The rest of the document is structured as follows. Section 2 talks about the changes to authentication mode as described in BFD [RFC5880]. Section 3 goes into the details of the new Authentication Type.

1.1. Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

1.2. Terminology

The following terms used in this document have been defined in BFD [RFC5880].

- Detect Multiplier
- Detection Time

Term	Meaning
significant change	State change, a demand model change (to D bit) or a poll sequence change (P or F bit).
configured interval	configured authentication periodic interval

2. Authentication Mode

The cryptographic authentication mechanisms specified in BFD [RFC5880] describes enabling and disabling of authentication as a one time operation. As a security precaution, it mentions that authentication state be allowed to change at most once. Once enabled, every packet must have Authentication Bit set and the

associated Authentication Type appended. In addition, it states that an implementation SHOULD NOT allow the authentication state to be changed based on the receipt of a BFD Control packet.

This document proposes that the authentication mode be modified to be enabled on demand. Instead of authenticating every packet, BFD peers are configured for which packets need to be authenticated, and authenticate only those packets. Rest of the packets can be transmitted and received without authentication. For example, the two ends can be configured such that BFD packets that indicate a significant change should be authenticated and enable authentication on those packets only. If the two ends have previously been configured as such, but at least one side decides not to authenticate a significant change frame, then the BFD session will fail to come up.

This proposal outlines which packets need to be authenticated (carry the A-bit), and which packets can be transmitted or received without authentication enabled. A frame that fails authentication is discarded, or a frame that was supposed to be authenticated, but was not, e.g. a significant change frame, is discarded. However, there is no change to the state machine for BFD, as the decision of a significant change is still decided by how many valid consecutive packets were received, authenticated or otherwise.

The following table summarizes when the A bit should be set. The table should be read with the column indicating the BFD state the receiver is currently in, and the row indicating the BFD state the receiver might transition to based on the packet received. The interesection of the two indicates whether the received packet should have the A bit set (Auth), no authentication is needed (NULL), most packets are NULL AUTH (Select) or the state transition is not applicable.

Read   : On state change from <column> to <row>
Auth   : Authenticate frame
NULL   : No Authentication. Use NULL AUTH Type.
n/a   : Invalid state transition.
Select : Most packets NULL AUTH. Selective (periodic) packets authenticated.

	DOWN	INIT	UP	ADMIN DOWN
DOWN	NULL	Auth	Auth	NULL
INIT	Auth	NULL	n/a	n/a
UP	Auth	Auth	Select	n/a
ADMIN	NULL	Auth	Auth	NULL

Optimized Authentication Map

If P or F bit changes value, the packet MUST be authenticated. If the D bit changes value, the packet MUST be authenticated.

All packets already carry the sequence number. The NULL AUTH packets MUST contain the Type specified in Section 3. This enables a monotonically increasing sequence number to be carried in each frame, and prevents man-in-the-middle from capturing and replaying the same frame again. Since all packets still carry a sequence number, the logic for sequence number maintenance remains unchanged from BFD [RFC5880]. If at a later time, a different scheme is adopted for changing sequence number, e.g. Secure BFD Sequence Numbers [I-D.ietf-bfd-secure-sequence-numbers], this method can use the updated scheme without any impact.

Most packets transmitted on a BFD session are BFD UP packets. Authenticating a small subset of these packets, for example, a detect multiplier number of packets per configured period, significantly reduces the computational demand for the system while maintaining security of the session across the configured authentication periods. A minimum of Detect Multiplier packets MUST be transmitted per configured periodic authentication interval. This ensures that the BFD session should see at least one authenticated packet during that interval.

3. NULL Auth Type

This section describes a new Authentication Type as:

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|   Auth Type   |   Auth Len    |  Auth Key ID  |   Reserved    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                        Sequence Number                        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

                          NULL Auth Type
```

where:

Auth Type: The Authentication Type, which in this case is TBD (NULL, to be assigned by IANA)

Auth Len: The length of the NULL Auth Type, in bytes i.e. 8 bytes

Auth Key ID: The authentication key ID in use for this packet. Must be set to zero.

Reserved: This byte MUST be set to zero on transmit and ignored on receive.

Sequence Number: The sequence number for this packet. Implementation may use sequence numbers (bfd.XmitAuthSeq) as defined in BFD [RFC5880], or secure sequence numbers as defined in Secure BFD Sequence Numbers [I-D.ietf-bfd-secure-sequence-numbers].

The NULL Auth Type must be used for all packets that are not authenticated. This protects against replay-attacks by allowing the session to maintain an incrementing sequence number for all packets (authenticated and un-authenticated).

In the future, if a new scheme is adopted for changing the sequence number, this method can adopt the new scheme without any impact.

4. IANA Considerations

This document requests an update to the registry titled "BFD Authentication Types". IANA is requested to to assign a new BFD Auth Type for "NULL" (see Section 3).

Note to RFC Editor: this section may be removed on publication as an RFC.

5. Security Considerations

The approach described in this document enhances the ability to authenticate a BFD session by taking away the onerous requirement that every BFD control packet be authenticated. By authenticating packets that affect the state of the session, the security of the BFD session is maintained. In this mode, packets that are a significant change but are not authenticated, are dropped by the system. Therefore, a malicious user that tries to inject a non-authenticated packet, e.g. with a Down state to take a session down will fail. That combined with the proposal of using sequence number defined in Secure BFD Sequence Numbers [I-D.ietf-bfd-secure-sequence-numbers] further enhances the security of BFD sessions.

6. References

6.1. Normative References

[I-D.ietf-bfd-secure-sequence-numbers]
Jethanandani, M., Agarwal, S., Mishra, A., Saxena, A., and A. DeKok, "Secure BFD Sequence Numbers", draft-ietf-bfd-secure-sequence-numbers-05 (work in progress), February 2020.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC5880] Katz, D. and D. Ward, "Bidirectional Forwarding Detection (BFD)", RFC 5880, DOI 10.17487/RFC5880, June 2010, <https://www.rfc-editor.org/info/rfc5880>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

6.2. Informative References

[RFC1321] Rivest, R., "The MD5 Message-Digest Algorithm", RFC 1321, DOI 10.17487/RFC1321, April 1992, <https://www.rfc-editor.org/info/rfc1321>.

[RFC6151] Turner, S. and L. Chen, "Updated Security Considerations for the MD5 Message-Digest and the HMAC-MD5 Algorithms", RFC 6151, DOI 10.17487/RFC6151, March 2011, <https://www.rfc-editor.org/info/rfc6151>.

[RFC6194] Polk, T., Chen, L., Turner, S., and P. Hoffman, "Security Considerations for the SHA-0 and SHA-1 Message-Digest Algorithms", RFC 6194, DOI 10.17487/RFC6194, March 2011, <https://www.rfc-editor.org/info/rfc6194>.

[SHA-1-attack1]
Wang, X., Yin, Y., and H. Yu, "Finding Collisions in the Full SHA-1", 2005.

[SHA-1-attack2]
Wang, X., Yao, A., and F. Yao, "New Collision Search for SHA-1", 2005.

Authors' Addresses

Mahesh Jethanandani
Kloud Services
USA

Email: mjethanandani@gmail.com

Ashesh Mishra
SES Networks

Email: mishra.ashesh@gmail.com

Ankur Saxena
Ciena Corporation
3939 N 1st Street
San Jose, CA 95134
USA

Email: ankurpsaxena@gmail.com

Manav Bhatia
Nokia
Bangalore
India

Email: manav.bhatia@nokia.com