Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: December 6, 2019

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

June 4, 2019

Optimizing BFD Authentication
draft-ietf-bfd-optimizing-authentication-08

Abstract

This document describes an optimization to BFD Authentication as described in Section 6.7 of BFD RFC5880.

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.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on December 6, 2019.

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 computationally intensive process, making 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 [SHA-1-attack1] [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 frames that signal a state change in BFD be authenticated. Rest of the frames can be transmitted and received without authentication enabled. Most frames that are transmitted and received have no state change associated with them. Limiting authentication to frames that affect a BFD session state allows more sessions to be supported for

authentication. Moreover, most BFD frames that signal a state 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 non-state change frame 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 TLV.

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 TLV 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 frames need to be authenticated, and authenticate only those frames. Rest of the frames can be transmitted and received without authentication. For example, the two ends can be configured such that BFD frames that indicate a state change should be authenticated and enable authentication on those frames only. If the two ends have previously been configured as such, but at least one side decides not to authenticate a state change frame, then the BFD session will fail to come up.

This proposal outlines which frames need to be authenticated (carry the A-bit), and which frames 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 state-change frame, is discarded. However, there is no change to the state machine for BFD, as the decision of a state change is still decided by how many valid consecutive frames were received, authenticated or otherwise.

The state changes for which authentication is being suggested include:

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

	DOWN	INIT	UP	POLL	DEMAND
DOWN	NULL	Auth	Auth	Auth	Auth
INIT	Auth	NULL	Auth	Auth	Auth
UP	Auth	n/a	Select	Auth	Auth
POLL	Auth	n/a	Auth	Auth	Auth
DEMAND	Auth	Auth	Auth	Auth	Auth

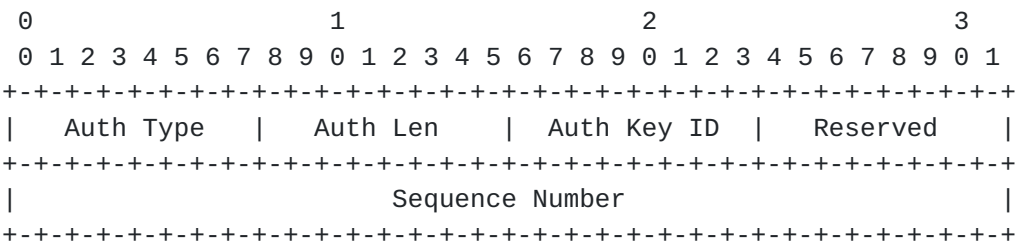
Optimized Authentication Map

All frames already carry the sequence number. The NULL AUTH frames MUST contain the TLV 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 frames still carry a sequence number, the logic for sequence number maintenance remains unchanged from [RFC5880]. If at a later time, a different scheme is adopted for changing sequence number, this method can use the updated scheme without any impact.

Most frames transmitted on a BFD session are BFD CC UP frames. Authenticating a small subset of these frames, 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 TLV

This section describes a new Authentication TLV as:



NULL Auth TLV

where:

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

Auth Len: The length of the NULL Auth TLV, 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 as defined in [RFC5880], or secure sequence numbers as defined in [I-D.ietf-bfd-secure-sequence-numbers].

The NULL Auth TLV must be used for all frames that are not authenticated. This protects against replay-attacks by allowing the session to maintain an incrementing sequence number for all frames (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 Auth TLV" (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 authentication a BFD session by taking away the onerous requirement that every frame be authenticated. By authenticating frames that affect the state of the session, the security of the BFD session is maintained. As such this document does not change the security considerations for BFD.

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-03 (work in progress), February 2019.

[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>.

[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>.

[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>.

[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
VMware
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