Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: August 18, 2016

M. Jethanandani
Cisco Systems
A. Mishra
A. Saxena
Ciena Corporation
M. Bhatia
Ionos Networks

February 15, 2016

Optimizing BFD Authentication
draft-ietf-bfd-optimizing-authentication-01

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 RFC 2119 [RFC2119].

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 http://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 August 18, 2016.

Copyright Notice

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.

Section 2 talks about the changes to authentication mode as described in BFD [RFC5880].

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 decide which frames need to be authenticated, and authenticate only those frames. For example, the two ends can decide that BFD frames that indicate a state change should be authenticated and enable authentication on those frames only. If the two ends have not previously negotiated which frames they will transmit or receive with authentication enabled, then the BFD session will fail to come up, because at least one end will expect every frame to be authenticated. 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

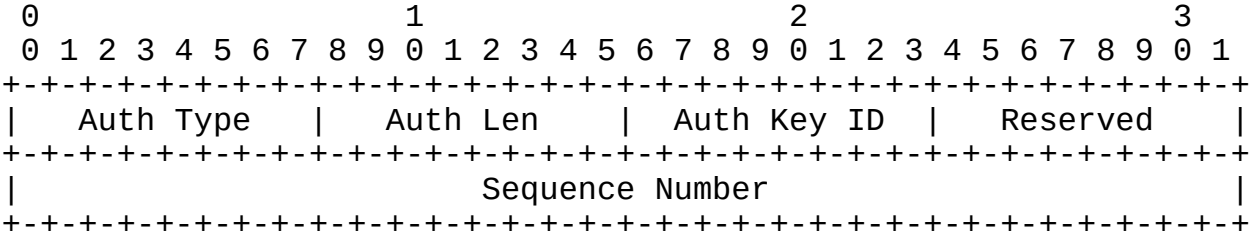
All frames already carry the sequence number. The NULL AUTH frames MUST contain the TLV specified in Section 3. This enables a monotonically increasing sequence number to be carried in each frame,

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].

Most frames transmitted on a BFD session are BFD CC UP frames. Authenticating a small subset of these frames (one per configured period) significantly reduces the computational demand for the system while maintaining security of the session across the configured authentication periods. The configuration of the periodic authentication interval for BFD CC UP frames is an open issue.

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 0 (NULL Auth TL)

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: The authentication key ID in use for this packet. This allows multiple keys to be active simultaneously.

Sequence Number: The sequence number for this packet. This value is incremented for each successive packet transmitted for a session. This provides protection against replay attacks. Must use the same sequence number counter as the authenticated frames.

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).

4. IANA Considerations

IANA is requested to assign a new Auth Type for the NULL Auth TLV.

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

[FIPS-180-2]
National Institute of Standards and Technology, FIPS PUB 180-2, "The Keyed-Hash Message Authentication Code (HMAC)", August 2002.

[FIPS-198]
National Institute of Standards and Technology, FIPS PUB 198, "The Keyed-Hash Message Authentication Code (HMAC)", March 2002.

[I-D.ashesh-bfd-stability]
Mishra, A., Jethanandani, M., Saxena, A., Networks, J., Chen, M., and P. Fan, "BFD Stability", draft-ashesh-bfd-stability-03 (work in progress), June 2015.

[I-D.ietf-bfd-generic-crypto-auth]
Bhatia, M., Manral, V., Zhang, D., and M. Jethanandani, "BFD Generic Cryptographic Authentication", draft-ietf-bfd-generic-crypto-auth-06 (work in progress), April 2014.

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

[RFC6039] Manral, V., Bhatia, M., Jaeggli, J., and R. White, "Issues with Existing Cryptographic Protection Methods for Routing Protocols", RFC 6039, DOI 10.17487/RFC6039, October 2010, <http://www.rfc-editor.org/info/rfc6039>.

[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, <http://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, <http://www.rfc-editor.org/info/rfc6194>.

6.2. Informative References

[Dobb96a] Dobbertin, H., "Cryptanalysis of MD5 Compress", May 1996.

[Dobb96b] Dobbertin, H., "The Status of MD5 After a Recent Attack", CryptoBytes", 1996.

[I-D.ietf-karp-design-guide] Lebovitz, G. and M. Bhatia, "Keying and Authentication for Routing Protocols (KARP) Design Guidelines", draft-ietf-karp-design-guide-10 (work in progress), December 2011.

[MD5-attack] Wang, X., Feng, D., Lai, X., and H. Yu, "Collisions for Hash Functions MD4, MD5, HAVAL-128 and RIPEMD", August 2004.

[NIST-HMAC-SHA] National Institute of Standards and Technology, Available online at http://csrc.nist.gov/groups/ST/hash/policy.html, "NIST's Policy on Hash Functions", 2006.

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

[RFC2104] Krawczyk, H., Bellare, M., and R. Canetti, "HMAC: Keyed-Hashing for Message Authentication", RFC 2104, DOI 10.17487/RFC2104, February 1997, <http://www.rfc-editor.org/info/rfc2104>.

[RFC4086] Eastlake 3rd, D., Schiller, J., and S. Crocker, "Randomness Requirements for Security", BCP 106, RFC 4086, DOI 10.17487/RFC4086, June 2005, <http://www.rfc-editor.org/info/rfc4086>.

[RFC4822] Atkinson, R. and M. Fanto, "RIPv2 Cryptographic Authentication", RFC 4822, DOI 10.17487/RFC4822, February 2007, <http://www.rfc-editor.org/info/rfc4822>.

[RFC5310] Bhatia, M., Manral, V., Li, T., Atkinson, R., White, R., and M. Fanto, "IS-IS Generic Cryptographic Authentication", RFC 5310, DOI 10.17487/RFC5310, February 2009, <http://www.rfc-editor.org/info/rfc5310>.

[RFC5709] Bhatia, M., Manral, V., Fanto, M., White, R., Barnes, M., Li, T., and R. Atkinson, "OSPFv2 HMAC-SHA Cryptographic Authentication", RFC 5709, DOI 10.17487/RFC5709, October 2009, <http://www.rfc-editor.org/info/rfc5709>.

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

[RFC6234] Eastlake 3rd, D. and T. Hansen, "US Secure Hash Algorithms (SHA and SHA-based HMAC and HKDF)", RFC 6234, DOI 10.17487/RFC6234, May 2011, <http://www.rfc-editor.org/info/rfc6234>.

[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
Cisco Systems
170 W. Tasman Drive
San Jose, CA 95134
USA

Phone: +1 (408) 526-8763
Email: mjethanandani@gmail.com

Ashesh Mishra
Ciena Corporation
3939 North 1st Street
San Jose, CA 95134
USA

Email: mishra.ashesh@gmail.com

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

Email: ankurpsaxena@gmail.com

Manav Bhatia
Ionos Networks
Bangalore
India

Email: manav@ionosnetworks.com