Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: November 25, 2014

D. Zhang
Huawei
M. Bhatia
Alcatel-Lucent
V. Manral
Ionos Networks
M. Jethanandani
Ciena Corporation

May 24, 2014

Authenticating BFD using HMAC-SHA-2 procedures
draft-ietf-bfd-hmac-sha-05

Abstract

This document describes the mechanism to authenticate Bidirectional Forwarding Detection (BFD) protocol packets using Hashed Message Authentication Mode (HMAC) with the SHA-256, SHA-384, and SHA-512 algorithms. The described mechanism uses the Generic Cryptographic Authentication and Generic Meticulous Cryptographic Authentication sections to carry the authentication data. This document updates, but does not supersede, the cryptographic authentication mechanism specified in RFC 5880.

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].

Table of Contents

1. Introduction

The cryptographic authentication mechanisms specified in BFD [RFC5880] defines MD5 Message-Digest Algorithm [RFC1321] and Secure Hash Algorithm (SHA-1) algorithms to authenticate BFD packets. 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].

These attacks may not necessarily result in direct vulnerabilities for Keyed-MD5 and Keyed-SHA-1 digests as message authentication codes because the colliding message may not correspond to a syntactically correct BFD protocol packet. Regardless, there is a need felt to deprecate MD5 and SHA-1 as the basis for the HMAC algorithm in favor of stronger digest algorithms.

This document adds support for Secure Hash Algorithms (SHA) defined in the US NIST Secure Hash Standard (SHS), which is defined by NIST FIPS 180-2 [FIPS-180-2]. [FIPS-180-2] includes SHA-1, SHA-224, SHA-256, SHA-384, and SHA-512. The HMAC authentication mode defined in NIST FIPS 198 is used [FIPS-198].

It is believed that the HMAC algorithms defined in HMAC: Keyed-Hashing for Message Authentication [RFC2104] is mathematically identical to their counterparts in [FIPS-198] and it is also believed that algorithms in US Secure Hash Algorithms [RFC6234] are mathematically identical to those defined in [FIPS-180-2].

It should be noted that the collision attacks currently known against SHA-1 do not apply when SHA-1 is used in the HMAC construction. NIST will be supporting HMAC-SHA-1 even after 2010 [NIST-HMAC-SHA] , whereas it would be dropping support for SHA-1 in digital signatures.

BFD Generic Cryptographic Authentication [I-D.ietf-bfd-generic-crypto-auth] defines new authentication types - Generic Cryptographic Authentication (TBD1) and Generic Meticulous Cryptographic Authentication (TBD2) that can be used for carrying the authentication digests defined in this document. Also please refer to this document for the procedures at the sending and the receiving side.

Implementations of this specification must include support for at least HMAC-SHA-256 and may include support for either of HMAC-SHA-384 or HMAC-SHA-512.

2. Cryptographic Aspects

In the algorithm description below, the following nomenclature, which is consistent with [FIPS-198], is used.

H is the specific hashing algorithm (e.g. SHA-256).

K is the password for the BFD packet.

Ko is the cryptographic key used with the hash algorithm.

B is the block size of H, measured in octets rather than bits. Note, that B is the internal block size, not the hash size. For SHA-1 and SHA-256 B is equal to 64. For SHA-384 and SHA-512 B is equal to 128.

L is the length of the hash, measured in octets rather than bits.

XOR is the exclusive-or operation.

Opad is the hexadecimal value 0x5c repeated B times.

Ipad is the hexadecimal value 0x36 repeated B times.

Apad is the hexadecimal value 0x878FE1F3 repeated (L/4) times.

2.1. Preperation of the Key

In this application, Ko is always L octets long.

If the Authentication Key (K) is L octets long, then Ko is equal to K. If the Authentication Key (K) is more than L octets long, then Ko is set to H(K). If the Authentication Key (K) is less than L octets long, then Ko is set to the Authentication Key (K) with zeros appended to the end of the Authentication Key (K) such that Ko is L octets long.

2.2. First Hash

First, the Authentication Data field in the Generic Authentication Section is filled with the value of Apad and the Authentication Type field is set to TBD1 or TBD2 depending upon which Authentication Type being used. The Sequence Number field MUST be set to bfd.XmitAuthSeq.

Then, a first hash, also known as the inner hash, is computed as follows:

First-Hash = H(Ko XOR Ipad || (BFD Packet))

2.3. Second Hash T

Then a second hash, also known as the outer hash, is computed as follows:

Second-Hash = H(Ko XOR Opad || First-Hash)

2.4. Result

The resultant Second-Hash becomes the Authentication Data that is sent in the Authentication Data field of the BFD Authentication Section. The length of the Authentication Data field is always identical to the message digest size of the specific hash function H that is being used.

This also means that the use of hash functions with larger output sizes will also increase the size of BFD Packet as transmitted on the wire.

3. IANA Considerations

This document makes no request of IANA.

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

4. Security Considerations

The approach described in this document enhances the security of the BFD protocol by adding, to the existing BFD cryptographic authentication methods, support for the SHA-2 algorithms defined in the NIST Secure Hash Standard (SHS) using the HMAC mode. However, the confidentiality protection for BFD packets is out of scope of this work .

Because all of the currently specified algorithms use symmetric cryptography, one cannot authenticate precisely which BFD device sent a given packet. However, one can authenticate that the sender knew the BFD Security Association (including the BFD SA's parameters) currently in use.

To enhance system security, the applied keys should be changed periodically and implementations SHOULD be able to store and use more than one key at the same time. The quality of the security provided by the cryptographic authentication option depends completely on the strength of the cryptographic algorithm and cryptographic mode in use, the strength of the key being used, and the correct implementation of the security mechanism in all communicating BFD implementations. Accordingly, the use of high assurance development methods is recommended. It also requires that all parties maintain the secrecy of the shared secret key. Randomness Requirements for Security [RFC4086] provides guidance on methods for generating cryptographically random bits.

The value Apad is used here primarily for consistency with IETF specifications for HMAC-SHA authentication for RIPv2 RIPv2 Cryptographic Authentication [RFC4822], IS-IS IS-IS Generic Cryptographic Authentication [RFC5310] and OSPFv2 OSPFv2 HMAC-SHA Cryptographic Authentication [RFC5709].

5. References

5.1. 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.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, March 1997.

[RFC6039] Manral, V., Bhatia, M., Jaeggli, J., and R. White, "Issues with Existing Cryptographic Protection Methods for Routing Protocols", RFC 6039, October 2010.

[RFC6151] Turner, S. and L. Chen, "Updated Security Considerations for the MD5 Message-Digest and the HMAC-MD5 Algorithms", RFC 6151, March 2011.

[RFC6194] Polk, T., Chen, L., Turner, S., and P. Hoffman, "Security Considerations for the SHA-0 and SHA-1 Message-Digest Algorithms", RFC 6194, March 2011.

5.2. 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, April 1992.

[RFC2104] Krawczyk, H., Bellare, M., and R. Canetti, "HMAC: Keyed-Hashing for Message Authentication", RFC 2104, February 1997.

[RFC4086] Eastlake, D., Schiller, J., and S. Crocker, "Randomness Requirements for Security", BCP 106, RFC 4086, June 2005.

[RFC4822] Atkinson, R. and M. Fanto, "RIPv2 Cryptographic Authentication", RFC 4822, February 2007.

[RFC5310] Bhatia, M., Manral, V., Li, T., Atkinson, R., White, R., and M. Fanto, "IS-IS Generic Cryptographic Authentication", RFC 5310, February 2009.

[RFC5709] Bhatia, M., Manral, V., Fanto, M., White, R., Barnes, M., Li, T., and R. Atkinson, "OSPFv2 HMAC-SHA Cryptographic Authentication", RFC 5709, October 2009.

[RFC5880] Katz, D. and D. Ward, "Bidirectional Forwarding Detection (BFD)", RFC 5880, June 2010.

[RFC6234] Eastlake, D. and T. Hansen, "US Secure Hash Algorithms (SHA and SHA-based HMAC and HKDF)", RFC 6234, May 2011.

[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

Dacheng Zhang
Huawei
Beijing
China

Email: zhangdacheng@huawei.com

Manav Bhatia
Alcatel-Lucent
Bangalore 560045
India

Email: manav.bhatia@alcatel-lucent.com

Vishwas Manral
Ionos Networks
CA
USA

Email: vishwas@ionosnetworks.com

Mahesh Jethanandani
Ciena Corporation
3939 North 1st Street
San Jose, CA 95134
USA

Phone: +1 (408) 904-2160
Email: mjethanandani@gmail.com