Internet Engineering Task Force (IETF)
Request for Comments: 6668
Updates: 4253
Category: Standards Track
ISSN: 2070-1721

D. Bider
Bitvise Limited
M. Baushke
Juniper Networks, Inc.

July 2012

# SHA-2 Data Integrity Verification for the Secure Shell (SSH) Transport Layer Protocol

## Abstract

This memo defines algorithm names and parameters for use in some of the SHA-2 family of secure hash algorithms for data integrity verification in the Secure Shell (SSH) protocol. It also updates RFC 4253 by specifying a new RECOMMENDED data integrity algorithm.

## Status of This Memo

This is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 5741.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at http://www.rfc-editor.org/info/rfc6668.

## 1. Overview and Rationale

The Secure Shell (SSH) [RFC4251] is a very common protocol for secure remote login on the Internet. Currently, SSH defines data integrity verification using SHA-1 and MD5 algorithms [RFC4253]. Due to recent security concerns with these two algorithms ([RFC6194] and [RFC6151], respectively), implementors and users request support for data integrity verification using some of the SHA-2 family of secure hash algorithms.

### 1.1. Requirements Terminology

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 [RFC2119].

## 2. Data Integrity Algorithms

This memo adopts the style and conventions of [RFC4253] in specifying how the use of new data integrity algorithms are indicated in SSH.

The following new data integrity algorithms are defined:

| | | |
|---|---|---|
| hmac-sha2-256 | RECOMMENDED | HMAC-SHA2-256<br>(digest length = 32 bytes,<br>key length = 32 bytes) |
| hmac-sha2-512 | OPTIONAL | HMAC-SHA2-512<br>(digest length = 64 bytes,<br>key length = 64 bytes) |

Figure 1

The Hashed Message Authentication Code (HMAC) mechanism was originally defined in [RFC2104] and has been updated in [RFC6151].

The SHA-2 family of secure hash algorithms is defined in [FIPS-180-3].

Sample code for the SHA-based HMAC algorithms are available in [RFC6234]. The variants, HMAC-SHA2-224 and HMAC-SHA2-384 algorithms, were considered but not added to this list as they have the same computational requirements of HMAC-SHA2-256 and HMAC-SHA2-512, respectively, and do not seem to be much used in practice.

Test vectors for use of HMAC with SHA-2 are provided in [RFC4231]. Users, implementors, and administrators may choose to put these new MACs into the proposal ahead of the REQUIRED hmac-sha1 algorithm defined in [RFC4253] so that they are negotiated first.

## 3. IANA Considerations

This document augments the MAC Algorithm Names in [RFC4253] and [RFC4250].

IANA has updated the "Secure Shell (SSH) Protocol Parameters" registry with the following entries:

| MAC Algorithm Name | Reference | Note |
|---|---|---|
| hmac-sha2-256 | RFC 6668 | Section 2 |
| hmac-sha2-512 | RFC 6668 | Section 2 |

Figure 2

## 4. Security Considerations

The security considerations of RFC 4253 [RFC4253] apply to this document.

The National Institute of Standards and Technology (NIST) publications: NIST Special Publication (SP) 800-107 [800-107] and NIST SP 800-131A [800-131A] suggest that HMAC-SHA1 and HMAC-SHA2-256 have a security strength of 128 bits and 256 bits, respectively, which are considered acceptable key lengths.

Many users seem to be interested in the perceived safety of using the SHA2-based algorithms for hashing.

## 5. References

### 5.1. Normative References

[FIPS-180-3] National Institute of Standards and Technology (NIST), United States of America, "Secure Hash Standard (SHS)", FIPS PUB 180-3, October 2008, <http://csrc.nist.gov/publications/fips/fips180-3/fips180-3_final.pdf>.

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

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC4231] Nystrom, M., "Identifiers and Test Vectors for HMAC-SHA-224, HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512", RFC 4231, December 2005.

[RFC4253] Ylonen, T. and C. Lonvick, Ed., "The Secure Shell (SSH) Transport Layer Protocol", RFC 4253, January 2006.

## 5.2. Informative References

[800-107] National Institute of Standards and Technology (NIST), "Recommendation for Applications Using Approved Hash Algorithms", NIST Special Publication 800-107, February 2009, <http://csrc.nist.gov/publications/nistpubs/800-107/NIST-SP-800-107.pdf>.

[800-131A] National Institute of Standards and Technology (NIST), "Transitions: Recommendation for the Transitioning of the Use of Cryptographic Algorithms and Key Lengths", DRAFT NIST Special Publication 800-131A, January 2011, <http://csrc.nist.gov/publications/nistpubs/800-131A/sp800-131A.pdf>.

[RFC4250] Lehtinen, S. and C. Lonvick, Ed., "The Secure Shell (SSH) Protocol Assigned Numbers", RFC 4250, January 2006.

[RFC4251] Ylonen, T. and C. Lonvick, Ed., "The Secure Shell (SSH) Protocol Architecture", RFC 4251, January 2006.

[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.

[RFC6234] Eastlake 3rd, D. and T. Hansen, "US Secure Hash Algorithms (SHA and SHA-based HMAC and HKDF)", RFC 6234, May 2011.

## Authors' Addresses

Denis Bider
Bitvise Limited
Suites 41/42, Victoria House
26 Main Street
GI

Phone: +1 869 762 1410
EMail: ietf-ssh2@denisbider.com
URI: http://www.bitvise.com/

Mark D. Baushke
Juniper Networks, Inc.
1194 N Mathilda Av
Sunnyvale, CA 94089-1206
US

Phone: +1 408 745 2952
EMail: mdb@juniper.net
URI: http://www.juniper.net/