Network Working Group
Internet-Draft
Updates: 4253 (if approved)
Intended status: Standards Track
Expires: July 26, 2012

d. bider
Bitvise Limited
M. Baushke
Juniper Networks, Inc.

January 23, 2012

SHA-2 Data Integrity Verification for the Secure Shell (SSH) Transport Layer Protocol
draft-dbider-sha2-mac-for-ssh-05

Abstract

This memo defines algorithm names and parameters for use of some of the SHA-2 family of secure hash algorithms for data integrity verification in the Secure Shell (SSH) protocol. It also updates RFC4253 by specifying a new RECOMMENDED data integrity algorithm.

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 July 26, 2012.

Copyright Notice

described in the Simplified BSD License.

1. Overview and Rationale

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 [RFC6151][RFC6194], implementors and users request support for data integrity verification using some of the SHA-2 family of of secure hash algorithms.

Please send comments on this draft to ietf-ssh@NetBSD.org.

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 defining new data integrity algorithms.

The following new data integrity algorithms are defined:

hmac-sha2-256	RECOMMENDED	HMAC-SHA2-256 (digest length = 32 bytes, key length = 32 bytes)
hmac-sha2-256-96	OPTIONAL	first 96 bits of HMAC-SHA2-256 (digest length = 12 bytes, key length = 32 bytes)
hmac-sha2-512	OPTIONAL	HMAC-SHA2-512 (digest length = 64 bytes, key length = 64 bytes)
hmac-sha2-512-96	OPTIONAL	first 96 bits of HMAC-SHA2-512 (digest length = 12 bytes, key length = 64 bytes)

Figure 1

The HMAC mechanism was originally defined in [RFC2104] and has been

updated in [RFC6151].

The SHA-2 family of secure hash algorithms are 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.

The truncated -96 OPTIONAL forms are present to allow applications which may be space restricted to still interoperate and make use of the new hashes.

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 would be negotiated first.

3. IANA Considerations

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

IANA is requested to update the SSH algorithm registry with the following entries:

MAC Algorithm Name	Reference	Note
hmac-sha2-256	This draft	Section 2
hmac-sha2-256-96	This draft	Section 2
hmac-sha2-512	This draft	Section 2
hmac-sha2-512-96	This draft	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, "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, "SSH Protocol Assigned Numbers", RFC 4250, January 2006.

[RFC4251] Ylonen, T. and C. Lonvick, "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, 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
Gibraltar
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/