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

Copyright Notice

Copyright (c) 2012 IETF Trust and the persons identified as the
document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust’s Legal
Provisions Relating to IETF Documents
(http://trustee.ietf.org/license-info) in effect on the date of
publication of this document. Please review these documents
carefully, as they describe your rights and restrictions with respect
to this document. Code Components extracted from this document must
include Simplified BSD License text as described in Section 4.e of
the Trust Legal Provisions and are provided without warranty as
described in the Simplified BSD License.
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
  (digest length = 32 bytes, key length = 32 bytes)
- hmac-sha2-512 OPTIONAL HMAC-SHA2-512
  (digest length = 64 bytes, 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-shal 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:

<table>
<thead>
<tr>
<th>MAC Algorithm Name</th>
<th>Reference</th>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>hmac-sha2-256</td>
<td>RFC 6668</td>
<td>Section 2</td>
</tr>
<tr>
<td>hmac-sha2-512</td>
<td>RFC 6668</td>
<td>Section 2</td>
</tr>
</tbody>
</table>

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


5.2. Informative References


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/