

Internet Engineering Task Force
Internet-Draft
Updates: [4253](#) (if approved)
Intended status: Standards Track
Expires: June 12, 2016

M. Baushke
Juniper Networks, Inc.
December 10, 2015

More Modular Exponential (MODP) Diffie-Hellman Groups for SSH
draft-baushke-ssh-dh-group-sha2-01

Abstract

This document defines two added Modular Exponential (MODP) Groups for the Secure Shell (SSH) protocol. It also updates [[RFC4253](#)] by specifying new RECOMMENDED and new OPTIONAL Diffie-Hellman key exchange algorithms using SHA-2 hashes.

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 June 12, 2016.

Copyright Notice

Copyright (c) 2015 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

Secure Shell (SSH) is a common protocol for secure communication on the Internet. In [\[RFC4253\]](#), SSH originally defined the Key Exchange Method Name `diffie-hellman-group1-sha1` which used [\[RFC2409\]](#) Oakley Group 1 (a MODP group with 768 bits) and SHA-1 [\[RFC3174\]](#). Due to recent security concerns with SHA-1 [\[RFC6194\]](#) and with MODP groups with less than 2048 bits [\[NIST-SP-800-131Ar1\]](#) implementors and users request support for larger MODP group sizes with data integrity verification using the SHA-2 family of secure hash algorithms as well as MODP groups providing more security.

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

2. 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 [\[RFC2119\]](#).

3. Key Exchange Algorithms

This memo adopts the style and conventions of [\[RFC4253\]](#) in specifying how the use of new data key exchange is indicated in SSH.

The following new key exchange algorithms are defined:

Key Exchange Method Name	Note
<code>diffie-hellman-group1-sha1</code>	NOT RECOMMENDED
<code>diffie-hellman-group14-sha256</code>	RECOMMENDED
<code>diffie-hellman-group15-sha256</code>	RECOMMENDED
<code>diffie-hellman-group16-sha256</code>	OPTIONAL

Figure 1

The SHA-2 family of secure hash algorithms are defined in [\[FIPS-180-4\]](#).

The method of key exchange used for the name `"diffie-hellman-group14-sha256"` is the same as that for `"diffie-hellman-group14-sha1"` except that the SHA2-256 hash algorithm is used.

The group15 and group16 names are the same as those specified in

[RFC3526] as 3072-bit MODP Group 14 and 4096-bit MODP Group 15.

4. IANA Considerations

This document augments the Key Exchange Method Names in [RFC4253].

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

Key Exchange Method Name	Reference	Note
diffie-hellman-group1-sha1	RFC4253	NOT RECOMMENDED
diffie-hellman-group14-sha256	This draft	RECOMMENDED
diffie-hellman-group15-sha256	This draft	RECOMMENDED
diffie-hellman-group16-sha256	This draft	OPTIONAL

Figure 2

It is RECOMMENDED that the new diffie-hellman-group14-sha256 method be proposed before the diffie-hellman-group14-sha1 method.

5. Security Considerations

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

The security considerations of [RFC3526] suggest that these MODP groups have security strengths given in this table.

Group modulus security strength estimates

Group	Modulus	Strength Estimate 1		Strength Estimate 2	
		in bits	exponent size	in bits	exponent size
14	2048-bit	110	220-	160	320-
15	3072-bit	130	260-	210	420-
16	4096-bit	150	300-	240	480-

+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+

Figure 3

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

6. References

Baushke

Expires June 12, 2016

[Page 3]

Internet-Draft

More MODP DH groups for SSH

December 2015

6.1. Normative References

[FIPS-180-4]

National Institute of Standards and Technology, "Secure Hash Standard (SHS)", FIPS PUB 180-4, August 2015, <<http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf>>.

[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>>.

[RFC3526] Kivinen, T. and M. Kojo, "More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE)", [RFC 3526](#), DOI 10.17487/RFC3526, May 2003, <<http://www.rfc-editor.org/info/rfc3526>>.

[RFC4253] Ylonen, T. and C. Lonvick, Ed., "The Secure Shell (SSH) Transport Layer Protocol", [RFC 4253](#), DOI 10.17487/RFC4253, January 2006, <<http://www.rfc-editor.org/info/rfc4253>>.

6.2. Informative References

[NIST-SP-800-131Ar1]

Barker, and Roginsky, "Transitions: Recommendation for the Transitioning of the Use of Cryptographic Algorithms and Key Lengths", NIST Special Publication 800-131A Revision 1, November 2015,

<<http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-131Ar1.pdf>>.

- [RFC2409] Harkins, D. and D. Carrel, "The Internet Key Exchange (IKE)", [RFC 2409](#), DOI 10.17487/RFC2409, November 1998, <<http://www.rfc-editor.org/info/rfc2409>>.
- [RFC3174] Eastlake 3rd, D. and P. Jones, "US Secure Hash Algorithm 1 (SHA1)", [RFC 3174](#), DOI 10.17487/RFC3174, September 2001, <<http://www.rfc-editor.org/info/rfc3174>>.
- [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>>.

Baushke

Expires June 12, 2016

[Page 4]

Internet-Draft

More MODP DH groups for SSH

December 2015

Author's Address

Mark D. Baushke
Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, CA 94089-1228
US

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

