Internet Engineering Task Force
Internet-Draft
Updates: 4253, 4419, 4432, 4462, 5656
(if approved)
Intended status: Standards Track
Expires: August 15, 2016

M. Baushke
Juniper Networks, Inc.

February 12, 2016

More Modular Exponential (MODP) Diffie-Hellman Groups for SSH
draft-baushke-ssh-dh-group-sha2-02

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 August 15, 2016.

Copyright Notice

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.

The United States Information Assurance Directorate at the National Security Agency has published a FAQ [MFQ-U-OO-815099-15] suggesting that the use of ECDH using the nistp256 curve and SHA-2 based hashes less than SHA2-384 are no longer sufficient for transport of Top Secret information. It is for this reason that this draft moves ecdh-sha2-nistp256 from a REQUIRED to OPTIONAL as a key exchange method. This is the same reason that the stronger MODP groups being introduced are using SHA2-512 as the hash algorithm. Group14 is already present in most SSH implementations and most implementations already have a SHA2-256 implementation, so diffie-hellman-group14-sha256 is provided as an easy to implement and faster to use key exchange for small embedded applications.

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
diffie-hellman-group14-sha256	MAY/OPTIONAL
diffie-hellman-group15-sha512	MUST/REQUIRED/SHALL
diffie-hellman-group16-sha512	SHOULD/RECOMMENDED
diffie-hellman-group17-sha512	MAY/OPTIONAL
diffie-hellman-group18-sha512	MAY/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 algorith is used.

The group15, group16, group17, and group18 names are the same as those specified in [RFC3526] as 3072-bit MODP Group 14, 4096-bit MODP Group 15, 6144-bit MODP Group 17, and 8192-bit MODP Group 18.

The SHA2-512 algorithm is to be used when "sha512" is specified as a part of the key exchange method name.

4. IANA Considerations

This document augments the Key Exchange Method Names in [RFC4253]. It downgrades the use of SHA-1 hashing for key exchange methods in [RFC4419], [RFC4432], and [RFC4462]. It also moves from MUST to MAY the ecdh-sha2-nistp256 given in [RFC5656].

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

Key Exchange Method Name	Reference	Note
diffie-hellman-group-exchange-sha1	RFC4419	SHOULD NOT
diffie-hellman-group-exchange-sha256	RFC4419	MAY
diffie-hellman-group1-sha1	RFC4253	SHOULD NOT
diffie-hellman-group14-sha1	RFC4253	MAY
ecdh-sha2-nistp256	RFC5656	MAY
ecdh-sha2-nistp384	RFC5656	MUST
ecdh-sha2-nistp521	RFC5656	MUST
ecdh-sha2-*	RFC5656	MAY
ecmqv-sha2	RFC5656	MAY
gss-gex-sha1-*	RFC4462	SHOULD NOT
gss-group1-sha1-*	RFC4462	SHOULD NOT
gss-group14-sha1-*	RFC4462	MAY
gss-*	RFC4462	MAY
rsa1024-sha1	RFC4432	SHOULD NOT
rsa2048-sha256	RFC4432	MAY
diffie-hellman-group14-sha256	This Draft	MAY
diffie-hellman-group15-sha512	This Draft	MUST
diffie-hellman-group16-sha512	This Draft	SHOULD
diffie-hellman-group17-sha512	This Draft	MAY
diffie-hellman-group18-sha512	This Draft	MAY

Figure 2

The SHA-1 hashing SHOULD NOT be used. If it is used, it should only be provided for backwards compatibility and should not be used in new

designs and should be phased out of existing key exchanges as quickly as possible because it is NOT SECURE. Any key exchange using SHA-1 SHOULD NOT be in a default key exchange list if at all possible. If they are needed for backward compatibility, they SHOULD be listed after all of the SHA-2 based key exchanges.

The RFC4253 REQUIRED diffie-hellman-group14-sha1 method MAY be retained for compatibility with older Secure Shell implementations. It is intended that this key exchange be phased out as soon as possible.

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-
17	6144-bit	170	340-	270	540-
18	8192-bit	190	380-	310	620-

Figure 3

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

6. References

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

[MFQ-U-OO-815099-15]
"National Security Agency/Central Security Service", "CNSA Suite and Quantum Computing FAQ", January 2016, <https://www.iad.gov/iad/library/ia-guidance/ia-solutions-for-classified/algorithm-guidance/cnsa-suite-and-quantum-computing-faq.cfm>.

[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>.

[RFC4419] Friedl, M., Provos, N., and W. Simpson, "Diffie-Hellman Group Exchange for the Secure Shell (SSH) Transport Layer Protocol", RFC 4419, DOI 10.17487/RFC4419, March 2006, <http://www.rfc-editor.org/info/rfc4419>.

[RFC4432] Harris, B., "RSA Key Exchange for the Secure Shell (SSH) Transport Layer Protocol", RFC 4432, DOI 10.17487/RFC4432, March 2006, <http://www.rfc-editor.org/info/rfc4432>.

[RFC4462] Hutzelman, J., Salowey, J., Galbraith, J., and V. Welch, "Generic Security Service Application Program Interface (GSS-API) Authentication and Key Exchange for the Secure Shell (SSH) Protocol", RFC 4462, DOI 10.17487/RFC4462, May 2006, <http://www.rfc-editor.org/info/rfc4462>.

[RFC5656] Stebila, D. and J. Green, "Elliptic Curve Algorithm Integration in the Secure Shell Transport Layer", RFC 5656, DOI 10.17487/RFC5656, December 2009, <http://www.rfc-editor.org/info/rfc5656>.

[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>.

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/