Internet Engineering Task Force
Internet-Draft
Updates: 4253, 4432, 4462 (if approved)
Intended status: Standards Track
Expires: March 15, 2017

M. Baushke
Juniper Networks, Inc.

September 11, 2016

More Modular Exponential (MODP) Diffie-Hellman (DH) Key Exchange (KEX) Groups for Secure Shell (SSH) draft-ietf-curdle-ssh-modp-dh-sha2-00

Abstract

This document defines added Modular Exponential (MODP) Groups for the Secure Shell (SSH) protocol 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 March 15, 2017.

Copyright Notice

1. Overview and Rationale

Secure Shell (SSH) is a common protocol for secure communication on the Internet. Due to recent security concerns with SHA-1 [RFC6194] and with MODP groups with less than 2048 bits [NIST-SP-800-131Ar1] implementer and users request support for larger Diffie Hellman (DH) 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 both: a) DH groups using less than 3072-bits, and b) the use of SHA-2 based hashes less than SHA2-384, are no longer sufficient for transport of Top Secret information. For this reason, the new MODP groups are being introduced starting with the MODP 3072-bit group 15 are all using SHA2-512 as the hash algorithm.

The DH 2048-bit MODP group 14 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.

In [RFC4462], there is another method for providing DH key exchange with MODP Groups using "Generic Security Service Application Program Interface (GSS-API)". This RFC extends the "gss-*" MODP DH groups and provides for using SHA-2 based hashes for them as well.

Please send comments on this draft to ietf-ssh@NetBSD.org and ietf-curdle@ietf.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
diffie-hellman-group14-sha256
diffie-hellman-group15-sha512
diffie-hellman-group16-sha512
diffie-hellman-group17-sha512
diffie-hellman-group18-sha512
gss-group14-sha256-*
gss-group15-sha512-*
gss-group16-sha512-*
gss-group17-sha512-*
gss-group18-sha512-*
```

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 method of key exchange used for the name "gss-group14-sha256-*" is the same as that for "gss-group14-sha1-*" except that the SHA2-256 hash algorithm is used.

The group15 through group18 names are the same as those specified in [RFC3526] 3071-bit MODP Group 15, 4096-bit MODP Group 16, 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].

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

Key Exchange Method Name	Reference	Note
diffie-hellman-group14-sha256	This Draft	MAY
diffie-hellman-group15-sha512	This Draft	MAY
diffie-hellman-group16-sha512	This Draft	MAY
diffie-hellman-group17-sha512	This Draft	MAY
diffie-hellman-group18-sha512	This Draft	MAY
gss-group14-sha256-*	This Draft	MAY
gss-group15-sha512-*	This Draft	MAY
gss-group16-sha512-*	This Draft	MAY
gss-group17-sha512-*	This Draft	MAY
gss-group18-sha512-*	This Draft	MAY

Figure 2

The Note in the above table is not an implementation suggestion/ recommendation for the listed key exchange method. It is up to the end-user as to what algorithms they choose to be able to negotiate. This RFC is intended to provide IANA defined names for these groups for interoperability.

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. They are based on [RFC3766] Determining Strengths For Public Keys Used For Exchanging Symmetric Keys.

Group modulus security strength estimates (RFC3526)

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 larger MODP groups and hashing with SHA2-based algorithms.

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>.

[RFC3766] Orman, H. and P. Hoffman, "Determining Strengths For Public Keys Used For Exchanging Symmetric Keys", BCP 86, RFC 3766, DOI 10.17487/RFC3766, April 2004, <http://www.rfc-editor.org/info/rfc3766>.

[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>.

[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/