Internet Engineering Task Force
Internet-Draft
Updates: 4250, 4253 (if approved)
Intended status: Standards Track
Expires: March 18, 2018

M. Baushke
Juniper Networks, Inc.
September 14, 2017

More Modular Exponential (MODP) Diffie-Hellman (DH) Key Exchange (KEX) Groups for Secure Shell (SSH) draft-ietf-curdle-ssh-modp-dh-sha2-08

Abstract

This document defines added Modular Exponential (MODP) Groups for the Secure Shell (SSH) protocol using SHA-2 hashes. This document updates RFC 4250. This document updates RFC 4253 including an errata fix for checking the Peer's DH Public Key.

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 https://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 18, 2018.

Copyright Notice

1. Overview and Rationale

Secure Shell (SSH) is a common protocol for secure communication on the Internet. Security protocols and primitives are an active area for research and help to suggest updates to SSH.

Section 3 of the [RFC4253] contains a small errata for checking the Peer's DH Public key. Section 4 of this document provides the correction.

Due to 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 use of larger MODP groups and the move to the SHA-2 family of hashes are important features to strengthen the key exchange algorithms available to the SSH client and server.

DH primes being adopted by this document are all "safe primes" such that p = 2q + 1 where q is also a prime. New MODP groups are being introduced starting with the MODP 3072-bit group 15. All use SHA512 as the hash algorithm.

The DH 2048-bit MODP group 14 is already present in most SSH implementations and most implementations already have a SHA256 implementation, so diffie-hellman-group14-sha256 is provided as easy to implement.

It is intended that these new MODP groups with SHA-2 based hashes update the [RFC4253] section 6.4 and [RFC4250] section 4.10 standards.

The United States Information Assurance Directorate (IAD) at the National Security Agency (NSA) has published "Commercial National Security Algorithm (CNSA) Suite and Quantum Computing Frequently Asked Questions (FAQ)" [MFQ-U-OO-815099-15] addressed to organizations that run classified or unclassified national security systems (NSS) and vendors that build products used in NSS.

This FAQ document indicates that NSS should no longer use:

- ECDH and ECDSA with NIST P-256
- SHA-256
- AES-128
- RSA with 2048-bit keys
- Diffie-Hellman with 2048-bit keys

The FAQ also states that NSS users should select DH groups based upon well established and validated parameter sets that comply with the minimum required sizes. Some specific examples include:

- Elliptic Curves are currently restricted to the NIST P-384 group only for both ECDH and ECDSA, in accordance with existing NIST and NIAP standards.
- RSA moduli should have a minimum size of 3072 bits (other than the noted PKI exception), and keys should be generated in accordance with all relevant NIST standards.
- For Diffie-Hellman use a Diffie-Hellman prime modulus of at least 3072 bits as specified in IETF RFC 3526 [RFC3526] (Groups 15-18).

Although SSH may not always be used to protect Top Secret communications, this document adopts the use of the DH groups

provided as an example in the FAQ as well as the use of SHA512 rather than SHA256 for the new DH groups.

[TO BE REMOVED: Please send comments on this draft to 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 RFC 2119 [RFC2119].

3. Key Exchange Algorithms

This document adds some new Key Exchange Algorithm Method Names in [RFC4253] and [RFC4250].

This document 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 method algorithms are defined:

- diffie-hellman-group14-sha256
- diffie-hellman-group15-sha512
- diffie-hellman-group16-sha512
- diffie-hellman-group17-sha512
- diffie-hellman-group18-sha512

The SHA-2 family of secure hash algorithms are defined in [RFC6234].

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 SHA256 hash algorithm is used. It is recommended that diffie-hellman-group14-sha256 SHOULD be supported to smooth the transition to newer group sizes.

The group15 through group18 names are the same as those specified in

[RFC3526] 3072-bit MODP Group 15, 4096-bit MODP Group 16, 6144-bit MODP Group 17, and 8192-bit MODP Group 18.

The SHA512 algorithm is to be used when "sha512" is specified as a part of the key exchange method name.

4. Checking the Peer's DH Public Key

Section 3 of [RFC4253] contains a small errata. When checking e (client public key) and f (server public key) values, an incorrect range is provided. The erroneous text is:

> Values of 'e' or 'f' that are not in the range [1, p-1] MUST NOT be sent or accepted by either side. If this condition is violated, the key exchange fails.

The errata is that the range should have been an open interval excluding the end point values. (i.e "(1, p-1)"). This document amends that document text as follows:

> DH Public key values MUST be checked and both conditions:
>
> 1 < e < p-1
>
> 1 < f < p-1
>
> MUST be true. Values not within these bounds MUST NOT be sent or accepted by either side. If either one of these condition is violated, then the key exchange fails.

This simple check ensures:

- The remote peer behaves properly.
- The local system is not forced into the two-element subgroup.

5. IANA Considerations

IANA is requested to add to the Key Exchange Method Names algorithm registry [IANA-KEX] with the following entries:

Key Exchange Method Name	Reference

diffie-hellman-group14-sha256	This Draft
diffie-hellman-group15-sha512	This Draft
diffie-hellman-group16-sha512	This Draft
diffie-hellman-group17-sha512	This Draft
diffie-hellman-group18-sha512	This Draft

[TO BE REMOVED: This registration should take place at the following location: <http://www.iana.org/assignments/ssh-parameters/ssh-parameters.xhtml#ssh-parameters-16>]

6. Acknowledgements

Thanks to the following people for review and comments: Denis Bider, Peter Gutmann, Damien Miller, Niels Moeller, Matt Johnston, Iwamoto Kouichi, Dave Dugal, Daniel Migault, Anna Johnston, Ron Frederick, Rich Salz, Travis Finkenauer, Eric Rescorla.

7. Security Considerations

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

The security considerations of [RFC3526] suggest that MODP group14 through group18 have security strengths that range between 110 bits of security through 310 bits of security. They are based on [RFC3766] Determining Strengths For Public Keys Used For Exchanging

Symmetric Keys. Care should be taken to use sufficient entropy and/or DRBG algorithms to maximize the true security strength of the key exchange and ciphers selected.

Using a fixed set of Diffie-Hellman parameters makes them a high value target for pre-computation. Generating additional sets of primes to be used, or moving to larger values is a mitigation against this issue.

8. References

8.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119,

DOI 10.17487/RFC2119, March 1997,
<https://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, <https://www.rfc-editor.org/info/rfc3526>.

[RFC4250] Lehtinen, S. and C. Lonvick, Ed., "The Secure Shell (SSH) Protocol Assigned Numbers", RFC 4250, DOI 10.17487/RFC4250, January 2006, <https://www.rfc-editor.org/info/rfc4250>.

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

8.2. Informative References

[IANA-KEX]
Internet Assigned Numbers Authority (IANA), "Secure Shell (SSH) Protocol Parameters: Key Exchange Method Names", March 2017, <http://www.iana.org/assignments/ssh-parameters/ssh-parameters.xhtml#ssh-parameters-16>.

[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, <https://www.rfc-editor.org/info/rfc3766>.

[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, <https://www.rfc-editor.org/info/rfc6194>.

[RFC6234] Eastlake 3rd, D. and T. Hansen, "US Secure Hash Algorithms (SHA and SHA-based HMAC and HKDF)", RFC 6234, DOI 10.17487/RFC6234, May 2011, <https://www.rfc-editor.org/info/rfc6234>.

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/