More Modular Exponentiation (MODP) Diffie-Hellman (DH)
Key Exchange (KEK) Groups for Secure Shell (SSH)

Abstract

This document defines added Modular Exponentiation (MODP) groups for
the Secure Shell (SSH) protocol using SHA-2 hashes. This document
updates RFC 4250. This document updates RFC 4253 by correcting an
error regarding checking the Peer's DH Public Key.

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 7841.

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) 2017 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
(https://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.
Table of Contents

1. Overview and Rationale ............................................. 2
2. Requirements Language .............................................. 4
3. Key Exchange Algorithms ............................................ 4
4. Checking the Peer’s DH Public Key ................................. 5
5. IANA Considerations .................................................. 5
6. Security Considerations .............................................. 6
7. References ............................................................. 6
   7.1. Normative References .......................................... 6
   7.2. Informative References ........................................ 7
Acknowledgements ........................................................... 8
Author’s Address .......................................................... 8

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 8 of [RFC4253] contains a small error in point 3 regarding
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], implementers and users
should request support for larger Diffie-Hellman (DH) MODP group
sizes with data-integrity verification by using the SHA-2 family of
secure hash algorithms and by having MODP groups provide 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 group15. All use SHA512
as the hash algorithm.

The DH 2048-bit MODP group14 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 Section 6.4 of [RFC4253] and Section 4.10 of [RFC4250].
The United States Information Assurance Directorate (IAD) at the National Security Agency (NSA) has published "Commercial National Security Algorithm Suite and Quantum Computing Frequently Asked Questions". [MFQ-U-OO-815099-15] is 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:

- Elliptic Curve Diffie-Hellman (ECDH) and Elliptic Curve Digital Signature Algorithm (ECDSA) with NIST P-256. (For SSH, this would suggest avoiding [RFC5656] Key Exchange Algorithm "ecdh-sha2-nistp256" and Public Key Algorithm "ecdsa-sha2-nistp256").

- SHA-256 (For SSH, this would suggest avoiding any Key Exchange Method using SHA1, SHA224, or SHA256 in favor of using SHA384 or SHA512.)

- AES-128 (For SSH, this would suggest avoiding Encryption Algorithms [RFC4253] "aes128-cbc" and [RFC4344] "aes128-ctr").

- RSA with 2048-bit keys (For SSH, this would suggest avoiding [RFC4253] "ssh-rsa" using RSA with SHA1 as well as [RFC6187] "x509v3-rsa2048-sha256" as well as any other RSA key that has a length less than 3072-bits or uses a hash less than SHA384.)

- Diffie-Hellman with 2048-bit keys (For SSH, this would suggest avoiding use of [RFC4253] both of "diffie-hellman-group1-shal" and "diffie-hellman-group14-shal" as well as avoiding "diffie-hellman-group14-sha256" added by this document.)

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 National Information Assurance Partnership (NIAP) standards. (For SSH, this means using [RFC5656] "ecdh-sha2-nistp384" for key exchange and "ecdsa-sha2-nistp384" for Public Key Algorithm Names.)

- 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. (For bit sizes as specified in [RFC3526], this would allow for any of group15, group16, group17, group18 to be used.)

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.

2. Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

3. Key Exchange Algorithms

This document adds some new Key Exchange Algorithm Method Names to what originally appeared 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 is 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-shal" 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 group15, 4096-bit MODP group16, 6144-bit MODP group17, and 8192-bit MODP group18.
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 8 of [RFC4253] contains a small error in point 3. 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 problem is that the range should have been an open interval excluding the endpoint 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 conditions is violated, then the key exchange fails.

This simple check ensures that:

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

5. IANA Considerations

IANA has added the following entries to the "Key Exchange Method Names" registry [IANA-KEX]:

<table>
<thead>
<tr>
<th>Method Name</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>diffie-hellman-group14-sha256</td>
<td>RFC 8268</td>
</tr>
<tr>
<td>diffie-hellman-group15-sha512</td>
<td>RFC 8268</td>
</tr>
<tr>
<td>diffie-hellman-group16-sha512</td>
<td>RFC 8268</td>
</tr>
<tr>
<td>diffie-hellman-group17-sha512</td>
<td>RFC 8268</td>
</tr>
<tr>
<td>diffie-hellman-group18-sha512</td>
<td>RFC 8268</td>
</tr>
</tbody>
</table>
6.  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 "Determining Strengths For Public Keys Used For Exchanging Symmetric Keys" [RFC3766]. Care should be taken to use sufficient entropy and/or deterministic random-bit generator (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 mitigates this issue.

7.  References

7.1.  Normative References


7.2. Informative References


Acknowledgements

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

Author’s Address

Mark D. Baushke
Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, CA  94089-1228
United States of America

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