Workgroup: Network Working Group
Internet-Draft:
draft-harwood-krb-pkinit-dh-upsize-01
Updates: 4556 (if approved)
Published: 6 August 2021
Intended Status: Standards Track
Expires: 7 February 2022
Authors: R. Harwood
Red Hat, Inc.

Deprecate Use of 1024-bit Diffie-Hellman Moduli in Public Key Cryptography for Initial Authentication in Kerberos

Abstract

Public Key Cryptography for Initial Authentication in Kerberos (PKINIT) permits a client and a Kerberos Domain Controller (KDC) to use a Diffie-Hellman (DH) exchange to derive an encryption key. The group with minimum modulus size permitted for this exchange is 1024 bits, which recent security research has shown to provide insufficient protection against organizations with sufficient computing resources, such as state-sponsored actors. This document updates RFC 4556 to increase the minimum group size to 2048 bits and define permitted groups of size larger than 4096-bits.

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 7 February 2022.

Copyright Notice

Table of Contents

1. Introduction

[RFC4556] specified three permitted groups for DH, which have modulus sizes 1024, 2048, and 4096 bits, respectively. It requires implementation of the 1024-bit and 2048-bit groups, while the 4096-bit group is optional albeit recommended. This document updates [RFC4556] such that the 1024-bit group is no longer permitted and implementation of the 4096-bit group is required based on more recent understanding of DH group weaknesses [LOGJAM]. It also defines two larger groups for futureproofing.

2. Conventions used in this document

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. Modulus Size Increases

In 2015, [LOGJAM] showed by example that it is very possible to break 768-bit DH groups. The authors extend their method to 1024-bit DH groups as well, and their analysis shows breaking 1024-bit DH groups to be within the reach of state-sponsored actors (or others with that level of computing resources). Accordingly, this document prohibits the use of the previously permitted 1024-bit group and recommends the use of the 4096-bit group.

[RFC4556] specifies three groups that can be used for Diffie-Hellman (DH) [RFC2631] key exchange between the client and Kerberos Domain Controller (KDC) [RFC4120]: Oakley 1024-bit Modular Exponential (MODP) well-known group 2 from [RFC2412], Oakley 2048-bit MODP well-known group 14 from [RFC3526], and Oakley 4096-bit MODP well-known group 16 from [RFC3526]. Of the three, implementations were required to support the 1024-bit and 2048-bit groups, while the 4096-bit group was optional.

Specifically, this document updates [RFC4556] Section 3.2.1, Item 8, Paragraph 1 as follows:

* implementations MUST NOT support Oakley 1024-bit MODP well-known group 2 [RFC2412] or any other group with modulus size strictly less than 2048 bits

* implementations MAY support Oakley 2048-bit MODP well-known group 14 [RFC3526]

* implementations MUST support Oakley 4096-bit MODP well-known group 16 [RFC3526]

4. Additional Groups

For futureproofing, we define two additional DH groups with larger modulus size. Implementations MAY support 6114-bit MODP group 17 and/or 8192-bit MODP group 18, both as defined by [RFC3526].

5. Interoperability

[RFC4556] mandated the implementation of two groups (of modulus size 1024-bit and 2048-bit respectively). While this document prohibits use of the 1024-bit group, use of the 2048-bit group is still permitted. Thus, pre-existing implementations could use either that 2048-bit group or the optional 4096-bit group for communication with an implementation that conforms to this document.

[RFC4556] permits KDC policy to reject DH groups with error code KDC_ERR_DH_KEY_PARAMETERS_NOT_ACCEPTED. Conforming implementations are thus already prepared to handle group selection failure. Two major implementations of Kerberos, MIT krb5 and Heimdal, have a configuration option for group selection (pkinit_dh_min_bits). In particular, the default value has always been 2048 for MIT krb5, which added PKINIT support in 2007.

6. Security Considerations

The security considerations of [RFC4556] continue to apply. As that document states:

> Kerberos error messages are not integrity protected; as a result, the domain parameters sent by the KDC as TD-DH-PARAMETERS can be tampered with by an attacker so that the set of domain parameters selected could be either weaker or not mutually preferred. Local policy can configure sets of domain parameters acceptable locally, or disallow the negotiation of DH domain parameters.

By removing known-dangerous groups, this document attempts to mitigate this attack. This document also permits implementation of only the 4096-bit group, which would effectively disallow parameter negotiation. However, as the field remains unprotected, it is still subject to Denial of Service from tampering in transit.

7. IANA Considerations

There are no IANA actions requested by this document.

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>.

[RFC2412] Orman, H., "The OAKLEY Key Determination Protocol", RFC 2412, DOI 10.17487/RFC2412, November 1998, <https://www.rfc-editor.org/info/rfc2412>.

[RFC2631] Rescorla, E., "Diffie-Hellman Key Agreement Method", RFC 2631, DOI 10.17487/RFC2631, June 1999, <https://www.rfc-editor.org/info/rfc2631>.

[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>.

[RFC4120] Neuman, C., Yu, T., Hartman, S., and K. Raeburn, "The Kerberos Network Authentication Service (V5)", RFC 4120, DOI 10.17487/RFC4120, July 2005, <https://www.rfc-editor.org/info/rfc4120>.

[RFC4556] Zhu, L. and B. Tung, "Public Key Cryptography for Initial Authentication in Kerberos (PKINIT)", RFC 4556, DOI 10.17487/RFC4556, June 2006, <https://www.rfc-editor.org/info/rfc4556>.

8.2. Informative References

[LOGJAM]

Adrian, D., Bhargavan, K., Durumeric, Z., Gaudry, P., Green, M., Halderman, J., Heninger, N., Springall, D., Thome, E., Valenta, L., VanderSloot, B., Wustrow, E., Zanella-Beguelin, S., and P. Zimmermann, "Imperfect Forward Secrect: How Diffie-Hellman Fails in Practice", ACM Conference on Computer and Communications Security (CCS) 2015, DOI 10.1145/2810103.2813707, 2015 , <https://weakdh.org/imperfect-forward-secrecy-ccs15.pdf>.

Appendix A. Acknowledgments

This document builds on prior work by the IETF CURves, Deprecating and a Little more Encryption Working Group (curdle), especially that of Loganaden Velvindron and Mark D. Baushke.

Author's Address

Robbie Harwood
Red Hat, Inc.

Email: rharwood@redhat.com