ipsecme
Internet-Draft
Updates: 5996 (if approved)
Intended status: Standards Track
Expires: October 4, 2013

Y. Sheffer
Porticor
S. Fluhrer
Cisco
April 2, 2013

Additional Diffie-Hellman Tests for IKEv2
draft-ietf-ipsecme-dh-checks-01

Abstract

This document adds a small number of mandatory tests required for the secure operation of IKEv2 with elliptic curve groups. No change is required to IKE implementations that use modular exponential groups, other than a few rarely used so-called DSA groups. This document updates the IKEv2 protocol, RFC 5996.

Status of this Memo

Copyright Notice

Table of Contents

1. Introduction

IKEv2 [RFC5996] consists of the establishment of a shared secret using the Diffie-Hellman (DH) protocol, followed by authentication of the two peers. Existing implementations typically use modular exponential (MODP) DH groups, such as those defined in [RFC3526].

IKEv2 does not require that any tests be performed by a peer receiving a public Diffie-Hellman key from the other peer. This is fine for the common case of MODP groups. For other DH groups, when peers reuse DH values across multiple IKE sessions, the lack of tests by the recipient results in a potential vulnerability (see Section 3.1 for more details). In particular, this is true for elliptic curve groups whose use is becoming ever more popular. This document defines such tests for several types of DH groups.

1.1. 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].

2. Group Membership Tests

This section describes the tests that need to be performed by IKE peers receiving a Key Exchange (KE) payload. The tests are RECOMMENDED for all implementations, but only REQUIRED for those that reuse DH secret keys (as defined in [RFC5996], Sec. 2.12). The tests are listed here according to the DH group being used.

2.1. Regular MODP Groups

These are currently the most commonly used groups; all these groups have the property that (p-1)/2 is also prime; this section applies to any such MODP group. Each recipient MUST verify that the peer's public value r is in the legal range (1 < r < p-1). According to [Menezes], Sec 2.2, even with this check there remains the possibility of leaking a single bit of the secret exponent when DH keys are reused; this amount of leakage is insignificant.

See Section 4 for the specific groups covered by this section.

2.2. MODP Groups with Small Subgroups

[RFC5114] defines modular exponential groups with small subgroups; these are modular exponential groups with comparatively small subgroups, and all have (p-1)/2 composite. Sec. 2.1 of [Menezes]

describes some informational leakage from a small subgroup attack on these groups, if the DH private value is reused.

This leakage can be prevented if the recipient performs a test on the peer's public value, however this test is expensive (approximately as expensive as what reusing DH private values saves). In addition, the NIST standard [NIST-800-56A] requires that test (see section 5.6.2.4), hence anyone needing to conform to that standard will need to implement the test anyway.

Because of the above, the IKE implementation MUST choose between one of the following two options:

- It MUST check both that the peer's public value is in range (1 < r < p-1) and that r**q = 1 mod p (where q is the size of the subgroup, as listed in the RFC). DH private values MAY then be reused. This option is appropriate if conformance to [NIST-800-56A] is required.
- It MUST NOT reuse DH private values (that is, the DH private value for each DH exchange MUST be generated from a fresh output of a cryptographically secure random number generator), and it MUST check that the peer's public value is in range (1 < r < p-1). This option is more appropriate if conformance to [NIST-800-56A] is not required.

See Section 4 for the specific groups covered by this section.

2.3. Elliptic Curve Groups

IKEv2 can be used with elliptic curve groups defined over a field GF(p) [RFC5903] [RFC5114]. According to [Menezes], Sec. 2.3, there is some informational leakage possible. A receiving peer MUST check that its peer's public value is valid; that is, it is not the point-at-infinity, and that the x and y parameters from the peer's public value satisfy the curve equation, that is, y**2 = x**3 + ax + b mod p (where for groups 19, 20, 21, a=-3, and all other values of a, b and p for the group are listed in the RFC).

See Section 4 for the specific groups covered by this section.

2.4. Transition

Existing implementations of IKEv2 with ECDH groups MAY be modified to include the tests described in the current document, if they do not reuse DH keys with multiple peers. The tests can be considered as sanity checks, and will prevent the code having to handle inputs that it may not have been designed to handle.

ECDH implementations that do reuse DH keys MUST be enhanced to include the above tests.

2.5. Protocol Behavior

The recipient of a DH public key that fails one of the above tests can assume that the sender either is truly malicious or else it has a bug in its implementation. The recipient MAY respond with an unauthenticated INVALID_SYNTAX notification, and MUST immediately drop the IKE SA.

3. Security Considerations

This entire document is concerned with the IKEv2 security protocol and the need to harden it in some cases.

3.1. DH Key Reuse and Multiple Peers

This section describes the attack prevented by the tests defined here.

Suppose that IKE peer Alice maintains IKE security associations with peers Bob and Eve. Alice uses the same secret ECDH key for both SAs, which is allowed with some restrictions. If Alice does not implement these tests, Eve will be able to send a malformed public key, which would allow her to efficiently determine Alice's secret key (as described in Sec. 2 of [Menezes]). Since the key is shared, Eve will be able to obtain Alice's shared IKE SA key with Bob.

3.2. Groups not covered by this RFC

There are a number of group types that are not specifically addressed by this RFC. A document that defines such a group MUST describe the tests required by that group.

One specific type of group would be an even-characteristic elliptic curve group. Now, these curves have cofactors greater than 1; this leads to a possibility of some information leakage. There are several ways to address this information leakage, such as performing a test analogous to the test in section 2.2, or adjusting the ECDH operation to avoid this leakage (such as "ECC CDH", where the shared secret really is hxyG). Because the appropriate test depends on how the group is defined, we cannot document it in advance.

3.3. Behavior Upon Test Failure

The behavior recommended in Section 2.5 is in line with generic error treatment during the IKE_SA_INIT exchange, Sec. 2.21.1 of [RFC5996]. The sender is not required to send back an error notification, and the recipient cannot depend on this notification because it is unauthenticated. Thus, the notification is only useful to debug implementation errors.

On the other hand, the error notification is secure, in the sense that no secret information is leaked. All IKEv2 Diffie-Hellman groups are publicly known, and none of the tests defined here depend on any secret key. In fact the tests can all be performed by an eavesdropper.

4. IANA Considerations

This document requests that IANA should add a column named "Recipient Tests" to the IKEv2 DH Group Transform IDs Registry [IANA-DH-Registry].

This column should initially be populated as per the following table.

Number	Recipient Tests
1, 2, 5, 14, 15, 16, 17, 18	[current], Sec. 2.1
22, 23, 24	[current], Sec. 2.2
19, 20, 21, 25, 26	[current], Sec. 2.3

Note to RFC Editor: please replace [current] by the RFC number assigned to this document.

Future documents that define new DH groups for IKEv2 are REQUIRED to provide this information for each new group, possibly by referring to the current document.

5. Acknowledgements

We would like to thank Dan Harkins who initially raised this issue on the ipsec mailing list. Thanks to Tero Kivinen and Rene Struik for their useful comments.

The document was prepared using the lyx2rfc tool, created by Nico Williams.

6. References

6.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC5996] Kaufman, C., Hoffman, P., Nir, Y., and P. Eronen, "Internet Key Exchange Protocol Version 2 (IKEv2)", RFC 5996, September 2010.

6.2. Informative References

[RFC3526] Kivinen, T. and M. Kojo, "More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE)", RFC 3526, May 2003.

[RFC5114] Lepinski, M. and S. Kent, "Additional Diffie-Hellman Groups for Use with IETF Standards", RFC 5114, January 2008.

[RFC5903] Fu, D. and J. Solinas, "Elliptic Curve Groups modulo a Prime (ECP Groups) for IKE and IKEv2", RFC 5903, June 2010.

[NIST-800-56A] National Institute of Standards and Technology (NIST), "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography (Revised)", NIST PUB 800-56A, March 2007.

[Menezes] Menezes, A. and B. Ustaoglu, "On Reusing Ephemeral Keys In Diffie-Hellman Key Agreement Protocols", December 2008, <http://www.cacr.math.uwaterloo.ca/techreports/2008/cacr2008-24.pdf>.

[IANA-DH-Registry] IANA, "Internet Key Exchange Version 2 (IKEv2) Parameters, Transform Type 4 - Diffie-Hellman Group Transform IDs", Jan. 2005, <http://www.iana.org/assignments/ikev2-parameters/ikev2-parameters.xml#ikev2-parameters-8>.

Appendix A. Appendix: Change Log

Note to RFC Editor: please remove this section before publication.

A.1. -01

- Corrected an author's name that was misspelled.
- Added recipient behavior if a test fails, and the related security considerations.

A.2. -00

- First WG document.
- Clarified IANA actions.
- Discussion of potential future groups not covered here.
- Clarification re: practicality of recipient tests for DSA groups.

Authors' Addresses

Yaron Sheffer
Porticor
10 Yirmiyahu St.
Ramat HaSharon 47298
Israel

Email: yaronf.ietf@gmail.com

Scott Fluhrer
Cisco Systems
1414 Massachusetts Ave.
Boxborough, MA 01719
USA

Email: sfluhrer@cisco.com