Network Working Group Y. Nir
Internet-Draft Check Point
Intended status: Standards Track T. Kivinen
Expires: April 11, 2016 INSIDE Secure
October 9, 2015

Cryptographic Algorithms for Use in the Internet Key Exchange Version 2 (IKEv2)

draft-nir-ipsecme-rfc4307bis-00

Abstract

The IPsec series of protocols makes use of various cryptographic algorithms in order to provide security services. The Internet Key Exchange protocol provides a mechanism to negotiate which algorithms should be used in any given association. However, to ensure interoperability between disparate implementations, it is necessary to specify a set of mandatory-to-implement algorithms to ensure that there is at least one algorithm that all implementations will have available. This document defines the current set of algorithms that are mandatory to implement as part of IKEv2, as well as algorithms that should be implemented because they may be promoted to mandatory at some future time.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

The Internet Key Exchange protocol [RFC7296] provides for the negotiation of cryptographic algorithms between both endpoints of a cryptographic association. Different implementations of IPsec and IKE may provide different algorithms. However, the IETF desires that all implementations should have some way to interoperate. In particular, this requires that IKE define a set of mandatory-to-implement algorithms because IKE itself uses such algorithms as part of its own negotiations. This requires that some set of algorithms be specified as "mandatory-to-implement" for IKE.

The nature of cryptography is that new algorithms surface continuously and existing algorithms are continuously attacked. An algorithm believed to be strong today may be demonstrated to be weak tomorrow. Given this, the choice of mandatory-to-implement algorithm should be conservative so as to minimize the likelihood of it being compromised quickly. Thought should also be given to performance considerations as many uses of IPsec will be in environments where performance is a concern.

Finally, we need to recognize that the mandatory-to-implement algorithm(s) may need to change over time to adapt to the changing world. For this reason, the selection of mandatory-to-implement algorithms was removed from the main IKEv2 specification and placed in this document. As the choice of algorithm changes, only this document should need to be updated.

Ideally, the mandatory-to-implement algorithm of tomorrow should already be available in most implementations of IPsec by the time it is made mandatory. To facilitate this, we will attempt to identify those algorithms (that are known today) in this document. There is no guarantee that the algorithms we believe today may be mandatory in the future will in fact become so. All algorithms known today are subject to cryptographic attack and may be broken in the future.

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].

We define some additional terms here:

SHOULD+   This term means the same as SHOULD. However, it is likely that an algorithm marked as SHOULD+ will be promoted at some future time to be a MUST.

SHOULD-   This term means the same as SHOULD. However, an algorithm marked as SHOULD- may be deprecated to a MAY in a future version of this document.

MUST-   This term means the same as MUST. However, we expect at some point that this algorithm will no longer be a MUST in a future document. Although its status will be determined at a later time, it is reasonable to expect that if a future revision of a document alters the status of a MUST- algorithm, it will remain at least a SHOULD or a SHOULD-.

3. Algorithm Selection

3.1. IKEv2 Transform Type 1 Algorithms

The algorithms in the below table are negotiated in the SA payload and used in the ENCR payload. References to the specifications defining these algorithms and the ones in the following subsections are in the IANA registry [IKEV2-IANA]. Some of these algorithms are Authenticated Encryption with Associated Data (AEAD - [RFC5282]). Algorithms that are not AEAD MUST be used in conjunction with the integrity algorithms in Section 3.2.

Name	Status	AEAD?
ENCR_AES_CBC	MUST	No
ENCR_CHACHA20_POLY1305	SHOULD	Yes
AES-GCM with a 8 octet ICV	SHOULD	Yes
ENCR_AES_CCM_8	SHOULD	Yes
ENCR_3DES	MAY	No
ENCR_DES	MUST NOT	No

3.2. IKEv2 Transform Type 3 Algorithms

The algorithms in the below table are negotiated in the SA payload and used in the ENCR payload. References to the specifications defining these algorithms are in the IANA registry. When an AEAD algorithm (see Section 3.1) is used, no algorithm from this table needs to be used.

Name	Status
AUTH_HMAC_SHA2_256_128	MUST
AUTH_HMAC_SHA1_96	MUST-
AUTH_AES_XCBC_96	MAY
AUTH_HMAC_MD5_96	MAY

3.3. IKEv2 Transform Type 2 Algorithms

Transform Type 2 Algorithms are pseudo-random functions used to generate random values when needed.

Name	Status
PRF_HMAC_SHA2_256	MUST
PRF_HMAC_SHA1	MUST-
PRF_AES128_CBC	MAY
PRF_HMAC_MD5	MAY

3.4. Diffie-Hellman Groups

There are several Modular Exponential (MODP) groups and several Elliptic Curve groups (ECC) that are defined for use in IKEv2. They are defined in both the [IKEv2] base document and in extensions documents. They are identified by group number.

Number	Description	Status
14	2048-bit MODP Group	MUST
19	256-bit random ECP group	SHOULD
20	384-bit random ECP group	MAY
2	1024-bit MODP Group	SHOULD NOT

4. Security Considerations

The security of cryptographic-based systems depends on both the strength of the cryptographic algorithms chosen and the strength of the keys used with those algorithms. The security also depends on the engineering of the protocol used by the system to ensure that there are no non-cryptographic ways to bypass the security of the overall system.

This document concerns itself with the selection of cryptographic algorithms for the use of IKEv2, specifically with the selection of "mandatory-to-implement" algorithms. The algorithms identified in this document as "MUST implement" or "SHOULD implement" are not known to be broken at the current time, and cryptographic research so far leads us to believe that they will likely remain secure into the foreseeable future. However, this isn't necessarily forever. We would therefore expect that new revisions of this document will be issued from time to time that reflect the current best practice in this area.

5. IANA Considerations

This document makes no requests of IANA.

6. Acknowledgements

The first version of this document was RFC 4307 by Jeffrey I. Schiller of the Massachusetts Institute of Technology (MIT). Much of the text has been copied verbatim.

7. References

7.1. Normative References

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

[RFC7296] Kaufman, C., Hoffman, P., Nir, Y., Eronen, P., and T. Kivinen, "Internet Key Exchange Protocol Version 2 (IKEv2)", STD 79, RFC 7296, October 2014.

[RFC5282] Black, D. and D. McGrew, "Using Authenticated Encryption Algorithms with the Encrypted Payload of the Internet Key Exchange version 2 (IKEv2) Protocol", RFC 5282, DOI 10.17487/RFC5282, August 2008, <http://www.rfc-editor.org/info/rfc5282>.

7.2. Informative References

[IKEV2-IANA] "Internet Key Exchange Version 2 (IKEv2) Parameters", <http://www.iana.org/assignments/ikev2-parameters>.

Authors' Addresses

Yoav Nir
Check Point Software Technologies Ltd.
5 Hasolelim st.
Tel Aviv 6789735
Israel

EMail: ynir.ietf@gmail.com

Tero Kivinen
INSIDE Secure
Eerikinkatu 28
HELSINKI FI-00180
FI

EMail: kivinen@iki.fi