Internet Engineering Task Force (IETF)
Request for Comments: 6379
Obsoletes: 4869
Category: Informational
ISSN: 2070-1721

L. Law
J. Solinas
NSA

October 2011

Suite B Cryptographic Suites for IPsec

Abstract

This document proposes four cryptographic user interface suites ("UI suites") for IP Security (IPsec), similar to the two suites specified in RFC 4308. The four new suites provide compatibility with the United States National Security Agency's Suite B specifications. This document obsoletes RFC 4869, which presented earlier versions of these suites.

Status of This Memo

This document is not an Internet Standards Track specification; it is published for informational purposes.

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). Not all documents approved by the IESG are a candidate for any level of Internet Standard; see Section 2 of RFC 5741.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at http://www.rfc-editor.org/info/rfc6379.

Table of Contents

1. Introduction

[RFC4308] proposes two optional cryptographic user interface suites ("UI suites") for IPsec. The two suites, VPN-A and VPN-B, represent commonly used present day corporate VPN security choices and anticipated future choices, respectively. [RFC4869] proposed four new UI suites based on implementations of the United States National Security Agency's Suite B algorithms (see [SuiteB]).

As with the VPN suites, the Suite B suites are simply collections of values for some options in IPsec. Use of UI suites does not change the IPsec protocols in any way.

This document reduces the scope of the suites in [RFC4869] while retaining the original suite names. A detailed list of the changes is given in Section 6. This document obsoletes RFC 4869.

2. Requirements Terminology

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. New UI Suites

Each of the following UI suites provides choices for ESP (see [RFC4303]) and for Internet Key Exchange (IKEv2) (see [RFC5996]). The four suites are differentiated by the choice of cryptographic algorithm strengths, and a choice of whether the Encapsulating Security Payload (ESP) is to provide both confidentiality and integrity or integrity only. The suite names are based on the

Advanced Encryption Standard [AES] mode and AES key length specified for ESP.

IPsec implementations that use these UI suites MUST use the suite names listed here. IPsec implementations SHOULD NOT use names different than those listed here for the suites that are described, and MUST NOT use the names listed here for suites that do not match these values. These requirements are necessary for interoperability.

3.1. Suite "Suite-B-GCM-128"

This suite provides ESP integrity protection and confidentiality using 128-bit AES-GCM (see [RFC4106]). This suite or the following suite should be used when ESP integrity protection and encryption are both needed.

ESP:

Encryption	AES with 128-bit keys and 16-octet Integrity Check Value (ICV) in GCM mode [RFC4106]
Integrity	NULL

IKEv2:

Encryption	AES with 128-bit keys in CBC mode [RFC3602]
Pseudo-random function	HMAC-SHA-256 [RFC4868]
Integrity	HMAC-SHA-256-128 [RFC4868]
Diffie-Hellman group	256-bit random ECP group [RFC5903]

3.2. Suite "Suite-B-GCM-256"

This suite provides ESP integrity protection and confidentiality using 256-bit AES-GCM (see [RFC4106]). This suite or the preceding suite should be used when ESP integrity protection and encryption are both needed.

ESP:

Encryption	AES with 256-bit keys and 16-octet ICV in GCM mode [RFC4106]
Integrity	NULL

IKEv2:

Encryption	AES with 256-bit keys in CBC mode [RFC3602]
Pseudo-random function	HMAC-SHA-384 [RFC4868]
Integrity	HMAC-SHA-384-192 [RFC4868]
Diffie-Hellman group	384-bit random ECP group [RFC5903]

3.3. Suite "Suite-B-GMAC-128"

This suite provides ESP integrity protection using 128-bit AES-GMAC (see [RFC4543]) but does not provide confidentiality. This suite or the following suite should be used only when there is no need for ESP encryption.

ESP:

Encryption	NULL
Integrity	AES with 128-bit keys in GMAC mode [RFC4543]

IKEv2:

Encryption	AES with 128-bit keys in CBC mode [RFC3602]
Pseudo-random function	HMAC-SHA-256 [RFC4868]
Integrity	HMAC-SHA-256-128 [RFC4868]
Diffie-Hellman group	256-bit random ECP group [RFC5903]

3.4. Suite "Suite-B-GMAC-256"

This suite provides ESP integrity protection using 256-bit AES-GMAC (see [RFC4543]) but does not provide confidentiality. This suite or the preceding suite should be used only when there is no need for ESP encryption.

ESP:

Encryption	NULL
Integrity	AES with 256-bit keys in GMAC mode [RFC4543]

IKEv2:

Encryption	AES with 256-bit keys in CBC mode [RFC3602]
Pseudo-random function	HMAC-SHA-384 [RFC4868]
Integrity	HMAC-SHA-384-192 [RFC4868]
Diffie-Hellman group	384-bit random ECP group [RFC5903]

4. Security Considerations

This document inherits all of the security considerations of the IPsec and IKEv2 documents.

Some of the security options specified in these suites may be found in the future to have properties significantly weaker than those that were believed at the time this document was produced.

5. IANA Considerations

IANA maintains a registry called "Cryptographic Suites for IKEv1, IKEv2, and IPsec" (see [IANA-Suites]). The registry consists of a text string and an RFC number that lists the associated transforms. The four suites in this document have been listed with this document as the RFC reference. These entries will be updated upon approval of this document.

The updated values for the registry are:

Identifier	Defined in
Suite-B-GCM-128	RFC 6379
Suite-B-GCM-256	RFC 6379
Suite-B-GMAC-128	RFC 6379
Suite-B-GMAC-256	RFC 6379

6. Changes from RFC 4869

The changes from [RFC4869] are:

1. Removed definitions of the suites for IKEv1.

2. Removed IKE authentication methods from the suite definitions. These now appear in [RFC6380].

3. Removed the requirements on rekeying in IKEv2.

7. References

7.1. Normative References

[IANA-Suites] Internet Assigned Numbers Authority, "Cryptographic Suites for IKEv1, IKEv2, and IPsec", <http://www.iana.org/assignments/crypto-suites>.

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

[RFC3602] Frankel, S., Glenn, R., and S. Kelly, "The AES-CBC Cipher Algorithm and Its Use with IPsec", RFC 3602, September 2003.

[RFC4106] Viega, J. and D. McGrew, "The Use of Galois/Counter Mode (GCM) in IPsec Encapsulating Security Payload (ESP)", RFC 4106, June 2005.

[RFC4303] Kent, S., "IP Encapsulating Security Payload (ESP)", RFC 4303, December 2005.

[RFC4308] Hoffman, P., "Cryptographic Suites for IPsec", RFC 4308, December 2005.

[RFC4543] McGrew, D. and J. Viega, "The Use of Galois Message Authentication Code (GMAC) in IPsec ESP and AH", RFC 4543, May 2006.

[RFC4868] Kelly, S. and S. Frankel, "Using HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512 with IPsec", RFC 4868, May 2007.

[RFC4869] Law, L. and J. Solinas, "Suite B Cryptographic Suites for IPsec", RFC 4869, May 2007.

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

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

7.2. Informative References

[AES] U.S. Department of Commerce/National Institute of Standards and Technology, "Advanced Encryption Standard (AES)", FIPS PUB 197, November 2001, <http://csrc.nist.gov/publications/fips/index.html>.

[RFC6380] Burgin, K. and M. Peck, "Suite B Profile for Internet Protocol Security (IPsec)", RFC 6380, October 2011.

[SuiteB] U.S. National Security Agency, "NSA Suite B Cryptography", January 2009, <http://www.nsa.gov/ia/programs/suiteb_cryptography/>.

Authors' Addresses

Laurie E. Law
National Security Agency

EMail: lelaw@orion.ncsc.mil

Jerome A. Solinas
National Security Agency

EMail: jasolin@orion.ncsc.mil