L. Law, NSA
J. Solinas, NSA

INTERNET-DRAFT
Expires July 10, 2007

January 10, 2007

Suite B Cryptographic Suites for IPsec
<draft-solinas-ui-suites-01.txt>

{{{ RFC Editor: Please replace every occurrence of "RFC xxxx" and "[RFCxxxx]" with the RFC number that is assigned to draft-kelly-ipsec-ciph-sha2 once it is approved and published. }}}

Status of this Memo

Abstract

This document proposes four optional cryptographic user interface suites ("UI suites") for 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.

Table of Contents

1. Introduction. 2
2. Requirements Terminology. 2
3. New UI Suites 2
   3.1 Suite "Suite-B-GCM-128" 2
   3.2 Suite "Suite-B-GCM-256" 3
   3.3 Suite "Suite-B-GMAC-128". 4
   3.4 Suite "Suite-B-GMAC-256". 5
4. Security Considerations 5

5. IANA Considerations 6
6. References. 6
6.1 Normative 6
6.2. Informative 7

1. Introduction

RFC 4308 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. This document proposes 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.

2. Requirements Terminology

The key words "MUST", "MUST NOT", "SHOULD", "SHOULD NOT", and "MAY" 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 IKEv1 and IKEv2 (see [RFC2409] and [RFC4306]). The four suites are differentiated by the choice of cryptographic algorithm strengths and a choice of whether ESP is to provide both confidentiality and integrity or integrity only. The suite names are based on the AES mode and AES key length specified for ESP.

IPsec implementations that use these UI suites SHOULD 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 ICV in GCM mode [RFC4106]
Integrity	NULL

IKEv1:

Encryption	AES with 128-bit keys in CBC mode [RFC3602]
Pseudo-random function	HMAC-SHA-256 [RFCxxxx]
Hash	SHA-256 [FIPS-180-2]
Diffie-Hellman group	256-bit random ECP group [RFC4753]
Group Type	ECP

For IKEv1, Phase 1 SHOULD use Main mode. IKEv1 implementations MUST support pre-shared key authentication [RFC2409] for interoperability. The authentication method used with IKEv1 MAY be either pre-shared key [RFC2409] or ECDSA-256 [RFC4754].

IKEv2:

Encryption	AES with 128-bit keys in CBC mode [RFC3602]
Pseudo-random function	HMAC-SHA-256 [RFCxxxx]
Integrity	HMAC-SHA-256-128 [RFCxxxx]
Diffie-Hellman group	256-bit random ECP group [RFC4753]
Authentication	ECDSA-256 [RFC4754]

Rekeying of Phase 2 (for IKEv1) or the CREATE_CHILD_SA (for IKEv2) MUST be supported by both parties in this suite.

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

IKEv1:
  Encryption                    AES with 256-bit keys in CBC mode
                                  [RFC3602]
  Pseudo-random function        HMAC-SHA-384 [RFCxxxx]
  Hash                          SHA-384 [FIPS-180-2]
  Diffie-Hellman group          384-bit random ECP group [RFC4753]
  Group Type                    ECP
```

For IKEv1, Phase 1 SHOULD use Main mode. IKEv1 implementations MUST support pre-shared key authentication [RFC2409] for interoperability. The authentication method used with IKEv1 MAY be either pre-shared key [RFC2409] or ECDSA-384 [RFC4754].


```
IKEv2:
  Encryption                    AES with 256-bit keys in CBC mode
                                  [RFC3602]
  Pseudo-random function        HMAC-SHA-384 [RFCxxxx]
  Integrity                     HMAC-SHA-384-192 [RFCxxxx]
  Diffie-Hellman group          384-bit random ECP group [RFC4753]
  Authentication                ECDSA-384 [RFC4754]
```

Rekeying of Phase 2 (for IKEv1) or the CREATE_CHILD_SA (for IKEv2) MUST be supported by both parties in this suite.

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]

IKEv1:
  Encryption                    AES with 128-bit keys in CBC mode
```

	[RFC3602]
Pseudo-random function	HMAC-SHA-256 [RFCxxxx]
Hash	SHA-256 [FIPS-180-2]
Diffie-Hellman group	256-bit random ECP group [RFC4753]
Group Type	ECP

For IKEv1, Phase 1 SHOULD use Main mode. IKEv1 implementations MUST support pre-shared key authentication [RFC2409] for interoperability. The authentication method used with IKEv1 MAY be either pre-shared key [RFC2409] or ECDSA-256 [RFC4754].

IKEv2:

Encryption	AES with 128-bit keys in CBC mode [RFC3602]
Pseudo-random function	HMAC-SHA-256 [RFCxxxx]
Integrity	HMAC-SHA-256-128 [RFCxxxx]
Diffie-Hellman group	256-bit random ECP group [RFC4753]
Authentication	ECDSA-256 [RFC4754]

Rekeying of Phase 2 (for IKEv1) or the CREATE_CHILD_SA (for IKEv2) MUST be supported by both parties in this suite.

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]

IKEv1:

Encryption	AES with 256-bit keys in CBC mode [RFC3602]
Pseudo-random function	HMAC-SHA-384 [RFCxxxx]
Hash	SHA-384 [FIPS-180-2]
Diffie-Hellman group	384-bit random ECP group [RFC4753]
Group Type	ECP

For IKEv1, Phase 1 SHOULD use Main mode. IKEv1 implementations MUST support pre-shared key authentication [RFC2409] for interoperability. The authentication method used with IKEv1 MAY be either pre-shared key [RFC2409] or ECDSA-384 [RFC4754].

IKEv2:

Encryption	AES with 256-bit keys in CBC mode [RFC3602]
Pseudo-random function	HMAC-SHA-384 [RFCxxxx]
Integrity	HMAC-SHA-384-192 [RFCxxxx]
Diffie-Hellman group	384-bit random ECP group [RFC4753]
Authentication	ECDSA-384 [RFC4754]

Rekeying of Phase 2 (for IKEv1) or the CREATE_CHILD_SA (for IKEv2) MUST be supported by both parties in this suite.

4. Security Considerations

This document inherits all of the security considerations of the IPsec, IKEv1, and IKEv2 documents. See [CNSSP-15] for guidance on the use of AES in these suites for the protection of U.S. Government information.

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 has created and will maintain 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 new suites in this document should be added to this registry after RFC publication and approval by an expert designated by the IESG.

The new values for the registry are:

Identifier	Defined in
Suite-B-GCM-128	RFC draft-solinas-ui-suites-00.txt
Suite-B-GCM-256	RFC draft-solinas-ui-suites-00.txt
Suite-B-GMAC-128	RFC draft-solinas-ui-suites-00.txt
Suite-B-GMAC-256	RFC draft-solinas-ui-suites-00.txt

6. References

6.1 Normative

[FIPS-180-2] FIPS 180-2 with change notice, "Secure Hash Standard", National Institute of Standards and Technology, February 2004.

[IANA-Suites] Internet Assigned Numbers Authority, "Cryptographic Suites for IKEv1, IKEv2, and IPsec", January 5, 2006. (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.

[RFC2409] Harkins, D. and D. Carrel, "The Internet Key Exchange (IKE)", RFC 2409, November 1998.

[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.

[RFC4306] Kaufman, C., "Internet Key Exchange (IKEv2) Protocol", RFC 4306, 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.

[RFC4753] Fu, D. and J. Solinas, "ECP Groups for IKE and IKEv2",

RFC 4753, November 2006.

[RFC4754] Fu, D. and J. Solinas, "IKE and IKEv2 Authentication Using ECDSA", RFC 4754, November 2006.

[RFCxxxx] Kelly, S., and S. Frankel, "Using HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512 With IPsec", RFC xxxx, 2007.

6.2 Informative

[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)

[CNSSP-15] Committee on National Security Systems, "National Policy on the Use of the Advanced Encryption Standard (AES) to Protect National Security Systems and National Security Information", June 2003. (http://www.cnss.gov/Assets/pdf/cnssp_15_fs.pdf)

[IANA-IKEv1] Internet Assigned Numbers Authority, Internet Key Exchange (IKE) Attributes, 5 Jun 2006. (http://www.iana.org/assignments/ipsec-registry)

[IANA-IKEv2] Internet Assigned Numbers Authority, IKEv2 Parameters, 26 September 2006. (http://www.iana.org/assignments/ikev2-parameters)

[RFC4634] D. Eastlake 3rd and T. Hansen, "US Secure Hash Algorithms (SHA and HMAC-SHA)", RFC 4634, July 2006.

[SuiteB] U.S. National Security Agency, "Fact Sheet NSA Suite B Cryptography", July 2005. (http://www.nsa.gov/ia/industry/crypto_Suite_b.cfm?MenuID=10.2.7)

Authors' Addresses

Laurie E. Law
National Information Assurance Research Laboratory
National Security Agency
EMail: lelaw@orion.ncsc.mil

Jerome A. Solinas
National Information Assurance Research Laboratory
National Security Agency
EMail: jasolin@orion.ncsc.mil

Full Copyright Statement

Intellectual Property

Expires July 10, 2007