Suite B Cryptographic Suites for IPsec

Status of This Memo

This memo provides information for the Internet community. It does not specify an Internet standard of any kind. Distribution of this memo is unlimited.

Copyright Notice

Copyright (C) The IETF Trust (2007).

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 References ......................................6
   6.2. Informative References ....................................7
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. 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 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 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 Integrity Check Value (ICV) in GCM mode [RFC4106]
- Integrity: NULL
IKEv1:

Encryption: AES with 128-bit keys in CBC mode

Pseudo-random function: HMAC-SHA-256 [RFC4868]

Hash: SHA-256 [FIPS-180-2] [RFC4634]

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

Pseudo-random function: HMAC-SHA-256 [RFC4868]

Integrity: HMAC-SHA-256-128 [RFC4868]

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

Pseudo-random function: HMAC-SHA-384 [RFC4868]

Hash: SHA-384 [FIPS-180-2] [RFC4634]

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 [RFC4868]
   Integrity                    HMAC-SHA-384-192 [RFC4868]
   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 [RFC4868]
   Hash                         SHA-256 [FIPS-180-2] [RFC4634]
   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 [RFC4868]
   Integrity                    HMAC-SHA-256-128 [RFC4868]
   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 [RFC4868]
   Hash                        SHA-384 [FIPS-180-2] [RFC4634]
   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 [RFC4868]
   Integrity                   HMAC-SHA-384-192 [RFC4868]
   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 have been added to this registry after approval by an expert designated by the IESG.

The new values for the registry are:

<table>
<thead>
<tr>
<th>Identifier</th>
<th>Defined in</th>
</tr>
</thead>
<tbody>
<tr>
<td>Suite-B-GCM-128</td>
<td>RFC 4869</td>
</tr>
<tr>
<td>Suite-B-GCM-256</td>
<td>RFC 4869</td>
</tr>
<tr>
<td>Suite-B-GMAC-128</td>
<td>RFC 4869</td>
</tr>
<tr>
<td>Suite-B-GMAC-256</td>
<td>RFC 4869</td>
</tr>
</tbody>
</table>

6. References

6.1. Normative References


6.2. Informative References


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

Copyright (C) The IETF Trust (2007).

This document is subject to the rights, licenses and restrictions contained in BCP 78, and except as set forth therein, the authors retain all their rights.

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY, THE IETF TRUST AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Intellectual Property

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in BCP 78 and BCP 79.

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at http://www.ietf.org/ipr.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.

Acknowledgement

Funding for the RFC Editor function is currently provided by the Internet Society.