Network Working Group
Request for Comments: 4835
Obsoletes: 4305
Category: Standards Track

V. Manral
IP Infusion Inc.

April 2007

# Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)

## Status of This Memo



## Copyright Notice



## Abstract

The IPsec series of protocols makes use of various cryptographic algorithms in order to provide security services. The Encapsulating Security Payload (ESP) and the Authentication Header (AH) provide two mechanisms for protecting data being sent over an IPsec Security Association (SA). 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 mandatory-to-implement algorithms for ESP and AH as well as specifying algorithms that should be implemented because they may be promoted to mandatory at some future time.

Table of Contents

## 1. Introduction

The Encapsulating Security Payload (ESP) and the Authentication Header (AH) provide two mechanisms for protecting data being sent over an IPsec Security Association (SA) [RFC4301], [RFC4302]. 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 mandatory-to-implement algorithms for ESP and AH as well as specifying algorithms that should be implemented because they may be promoted to mandatory at some future time.

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 is not included in the main IPsec, ESP, or AH specifications. It is instead 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 such algorithms (as they are known today) in this document. There is no guarantee that the algorithms that we (today) believe 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. 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].

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, it is likely that an algorithm marked as SHOULD- will be deprecated to a MAY or worse in a future version of this document.

MUST- This term means the same as MUST. However, we expect that at some point in the future this algorithm will no longer be a MUST.

## 3. Algorithm Selection

For IPsec implementations to interoperate, they must support one or more security algorithms in common. This section specifies the security algorithm implementation requirements for standards-conformant ESP and AH implementations. The security algorithms actually used for any particular ESP or AH security association are determined by a negotiation mechanism, such as the Internet Key Exchange (IKE [RFC2409], [RFC4306]) or pre-establishment.

Of course, additional standard and proprietary algorithms beyond those listed below can be implemented.

### 3.1. Encapsulating Security Payload

The implementation conformance requirements for security algorithms for ESP are given in the tables below. See Section 2 for definitions of the values in the "Requirement" column.

#### 3.1.1. ESP Encryption and Authentication Algorithms

These tables list encryption and authentication algorithms for the IPsec Encapsulating Security Payload protocol.

| Requirement | Encryption Algorithm (notes) |
|---|---|
| MUST | NULL [RFC2410] (1) |
| MUST | AES-CBC with 128-bit keys [RFC3602] |
| MUST- | TripleDES-CBC [RFC2451] |
| SHOULD | AES-CTR [RFC3686] |
| SHOULD NOT | DES-CBC [RFC2405] (2) |

| Requirement | Authentication Algorithm (notes) |
|---|---|
| MUST | HMAC-SHA1-96 [RFC2404] (3) |
| SHOULD+ | AES-XCBC-MAC-96 [RFC3566] |
| MAY | NULL (1) |
| MAY | HMAC-MD5-96 [RFC2403] (4) |

Notes:

(1) Since ESP encryption is optional, support for the "NULL" algorithm is required to maintain consistency with the way services are negotiated. Note that while authentication and encryption can each be "NULL", they MUST NOT both be "NULL" [RFC4301].

(2) DES, with its small key size and publicly demonstrated and open-design special-purpose cracking hardware, is of questionable security for general use.

(3) Weaknesses have become apparent in SHA-1 [SHA1-COLL]; however, these should not affect the use of SHA1 with HMAC.

(4) Weaknesses have become apparent in MD5 [MD5-COLL]; however, these should not affect the use of MD5 with HMAC.

### 3.1.2. ESP Combined Mode Algorithms

As specified in [RFC4303], combined mode algorithms are supported that provide both confidentiality and authentication services. Support of such algorithms will require proper structuring of ESP implementations. Under many circumstances, combined mode algorithms provide significant efficiency and throughput advantages. Although there are no suggested or required combined algorithms at this time, AES-CCM [RFC4309] and AES-GCM [RFC4106] are of interest. AES-CCM has been adopted as the preferred mode in IEEE 802.11 [802.11i], and AES-GCM has been adopted as the preferred mode in IEEE 802.1ae [802.1ae].

## 3.2. Authentication Header

The implementation conformance requirements for security algorithms for AH are given below. See Section 2 for definitions of the values in the "Requirement" column. As you would suspect, all of these algorithms are authentication algorithms.

| Requirement | Algorithm (notes) |
|---|---|
| MUST | HMAC-SHA1-96 [RFC2404] (1) |
| SHOULD+ | AES-XCBC-MAC-96 [RFC3566] |
| MAY | HMAC-MD5-96 [RFC2403] (2) |

Note:

(1) Weaknesses have become apparent in SHA-1 [SHA1-COLL]; however, these should not affect the use of SHA1 with HMAC.

(2) Weaknesses have become apparent in MD5 [MD5-COLL]; however, these should not affect the use of MD5 with HMAC.

## 4. Security Considerations

The security of cryptography-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 and administration 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 ESP and AH, 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 is not 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. Acknowledgements

Much of the wording herein was adapted from RFC 4305, the parent document of this document. RFC 4305 itself borrows text from [RFC4307], "Cryptographic Algorithms for Use in the Internet Key Exchange Version 2", by Jeffrey I. Schiller.

Thanks to the following people for reporting or responding to reports of the errors in RFC 4305: Paul Hoffman, Stephen Kent, Paul Koning, and Lars Volker. Helpful Last-Call comments were received from Russ Housley, Elwyn Davies, Nicolas Williams, and Alfred Hoenes.

## 6. Changes from RFC 2402 and RFC 2406 to RFC 4305

[RFC2402] and [RFC2406] defined the IPsec Authentication Header and IPsec Encapsulating Security Payload. Each specified the implementation requirements for cryptographic algorithms for their respective protocols. They have now been replaced with [RFC4302] and [RFC4303], which do not specify cryptographic algorithm implementation requirements, and this document, which specifies such requirements for both [RFC4302] and [RFC4303].

The implementation requirements are compared below:

| Old Req. | Old RFC(s) | New Requirement | Algorithm (notes) |
|---|---|---|---|
| MUST | 2406 | SHOULD NOT | DES-CBC [RFC2405] (1) |
| MUST | 2402 2406 | MAY | HMAC-MD5-96 [RFC2403] |
| MUST | 2402 2406 | MUST | HMAC-SHA1-96 [RFC2404] |

Note:

(1) The IETF deprecated the use of single DES years ago and has not included it in any new standard for some time (see IESG note on the first page of [RFC2407]). [RFC4305] represented the first standards-track recognition of that deprecation by specifying that implementations SHOULD NOT provide single DES. The US Government National Institute of Standards and Technology (NIST) has formally recognized the weakness of single DES by a notice published [DES-WDRAW] proposing to withdraw it as a US Government Standard. Triple DES remains approved by both the IETF and NIST.

## 7. Changes from RFC 4305

This document obsoletes [RFC4305]. The document incorporates changes for the support for the NULL Authentication Algorithm making the support from a MUST to a MAY. This change is made to make this document consistent with [RFC4301]. Text for SHA-1 collision attacks as well as the future use of AES-GCM and AES-CCM is added.

The changed implementation requirement resulting from the above changes is listed below:

| Old Req. | Old RFC(s) | New Requirement | Algorithm (notes) |
|---|---|---|---|
| MUST | 2406 | MAY | NULL Authentication |
| MUST | 2406 | MUST | NULL Encryption |
| SHOULD+ | 4305 | MUST | AES-CBC Encryption |

# 8. References

## 8.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP14, RFC2119, March 1997.

[RFC2403] Madson, C. and R. Glenn, "The Use of HMAC-MD5-96 within ESP and AH", RFC 2403, November 1998.

[RFC2404] Madson, C. and R. Glenn, "The Use of HMAC-SHA-1-96 within ESP and AH", RFC 2404, November 1998.

[RFC2405] Madson, C. and N. Doraswamy, "The ESP DES-CBC Cipher Algorithm With Explicit IV", RFC 2405, November 1998.

[RFC2410] Glenn, R. and S. Kent, "The NULL Encryption Algorithm and Its Use With IPsec", RFC 2410, November 1998.

[RFC2451] Pereira, R. and R. Adams, "The ESP CBC-Mode Cipher Algorithms", RFC 2451, November 1998.

[RFC3566] Frankel, S. and H. Herbert, "The AES-XCBC-MAC-96 Algorithm and Its Use With IPsec", RFC 3566, September 2003.

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

[RFC3686] Housley, R., "Using Advanced Encryption Standard (AES) Counter Mode With IPsec Encapsulating Security Payload (ESP)", RFC 3686, January 2004.

[RFC4301] Kent, S. and K. Seo, "Security Architecture for the Internet Protocol", RFC 4301, December 2005.

[RFC4302] Kent, S., "IP Authentication Header", RFC 4302,

December 2005.

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

[RFC4305] Eastlake, D., "Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)", RFC 4305, December 2005.

## 8.2. Informative References

[802.11i] "LAN/MAN Specific Requirements Part 11: Wireless Medium Access Control (MAC) and physical layer (PHY) specifications", IEEE Standard Medium Access Control (MAC) Security, IEEE Std 802.11i, June 2004.

[802.1ae] "Media Access Control (MAC) Security", IEEE Standard Medium Access Control (MAC) Security, IEEE Std 802.1ae, June 2006.

[DES-WDRAW] "Announcing Proposed Withdrawal of Federal Information Processing Standard (FIPS) for the Data Encryption Standard (DES) and Request for Comments", FIPS Notice Docket No. 040602169-4169-01, July 2004.

[MD5-COLL] Klima, V., "Finding MD5 Collisions - a Toy For a Notebook", Cryptology ePrint Archive Medium Report 2005/075, March 2005.

[RFC2402] Kent, S. and R. Atkinson, "IP Authentication Header", RFC 2402, November 1998.

[RFC2406] Kent, S. and R. Atkinson, "IP Encapsulating Security Payload (ESP)", RFC 2406, November 1998.

[RFC2407] Piper, D., "The Internet IP Security Domain of Interpretation for ISAKMP", RFC 2407, November 1998.

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

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

[RFC4306] Kaufman, C., "Internet Key Exchange (IKEv2) Protocol", RFC 4306, December 2005.

[RFC4307] Schiller, J., "Cryptographic Algorithms for Use in the Internet Key Exchange Version 2 (IKEv2)", RFC 4307, December 2005.

[RFC4309] Housley, R., "Using Advanced Encryption Standard (AES) CCM Mode with IPsec Encapsulating Security Payload (ESP)", RFC 4309, December 2005.

[SHA1-COLL] Rijmen, V. and E. Oswald, "Update on SHA-1", Cryptology ePrint Archive Report 2005/010, January 2005.

## Author's Address

Vishwas Manral
IP Infusion Inc.
Bamankhola, Bansgali,
Almora, Uttarakhand 263601
India

Phone: +91-98456-61911
EMail: vishwas@ipinfusion.com

## Full Copyright Statement



## Intellectual Property



## Acknowledgement

Funding for the RFC Editor function is provided by the IETF Administrative Support Activity (IASA).