Internet Engineering Task Force (IETF)
Request for Comments: 7321
Obsoletes: 4835
Category: Standards Track
ISSN: 2070-1721
August 2014

D. McGrew
Cisco Systems
P. Hoffman
VPN Consortium

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

Abstract

This document updates the Cryptographic Algorithm Implementation Requirements for the Encapsulating Security Payload (ESP) and Authentication Header (AH). It also adds usage guidance to help in the selection of these algorithms.

ESP and AH protocols make use of various cryptographic algorithms to provide confidentiality and/or data origin authentication to protected data communications in the IP Security (IPsec) architecture. To ensure interoperability between disparate implementations, the IPsec standard specifies a set of mandatory-to-implement algorithms. This document specifies the current set of mandatory-to-implement algorithms for ESP and AH, specifies algorithms that should be implemented because they may be promoted to mandatory at some future time, and also recommends against the implementation of some obsolete algorithms. Usage guidance is also provided to help the user of ESP and AH best achieve their security goals through appropriate choices of cryptographic algorithms.

This document obsoletes RFC 4835.

Status of This Memo

Table of Contents

1. Introduction

The Encapsulating Security Payload (ESP) [RFC4303] and the Authentication Header (AH) [RFC4302] are the mechanisms for applying cryptographic protection to data being sent over an IPsec Security Association (SA) [RFC4301].

To ensure interoperability between disparate implementations, it is necessary to specify a set of mandatory-to-implement algorithms. This ensures that there is at least one algorithm that all implementations will have in common. This document specifies the current set of mandatory-to-implement algorithms for ESP and AH, specifies algorithms that should be implemented because they may be promoted to mandatory at some future time, and also recommends against the implementation of some obsolete algorithms. Usage guidance is also provided to help the user of ESP and AH best achieve their security goals through appropriate choices of mechanisms.

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.

The ESP and AH mandatory-to-implement algorithm(s) may need to change over time to adapt to new developments in cryptography. For this reason, the specification of the mandatory-to-implement algorithms is not included in the main IPsec, ESP, or AH specifications, but is instead placed in this document. 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, this document identifies such algorithms, as they are known today. There is no guarantee that the algorithms that we predict will be mandatory in the future will actually be so. All algorithms known today are subject to cryptographic attack and may be broken in the future.

1.1. Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

We define some additional keywords here:

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.

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.

2. Implementation Requirements

This section specifies the cryptographic algorithms that MUST be implemented, and provides guidance about ones that SHOULD or SHOULD NOT be implemented.

In the following sections, all AES modes are for 128-bit AES. 192-bit and 256-bit AES MAY be supported for those modes, but the requirements here are for 128-bit AES.

2.1. ESP Authenticated Encryption (Combined Mode Algorithms)

ESP combined mode algorithms provide both confidentiality and authentication services; in cryptographic terms, these are authenticated encryption algorithms [RFC5116]. Authenticated encryption transforms are listed in the ESP encryption transforms IANA registry.

Requirement	Authenticated Encryption Algorithm
SHOULD+	AES-GCM with a 16 octet ICV [RFC4106]
MAY	AES-CCM [RFC4309]

2.2. ESP Encryption Algorithms

Requirement	Encryption Algorithm
MUST	NULL [RFC2410]
MUST	AES-CBC [RFC3602]
MAY	AES-CTR [RFC3686]
MAY	TripleDES-CBC [RFC2451]
MUST NOT	DES-CBC [RFC2405]

2.3. ESP Authentication Algorithms

Requirement	Authentication Algorithm (notes)
MUST	HMAC-SHA1-96 [RFC2404]
SHOULD+	AES-GMAC with AES-128 [RFC4543]
SHOULD	AES-XCBC-MAC-96 [RFC3566]
MAY	NULL [RFC4303]

Note that the requirement level for NULL authentication depends on the type of encryption used. When using authenticated encryption from Section 2.1, the requirement for NULL encryption is the same as the requirement for the authenticated encryption itself. When using the encryption from Section 2.2, the requirement for NULL encryption is truly "MAY"; see Section 3 for more detail.

2.4. AH Authentication Algorithms

The requirements for AH are the same as for ESP Authentication Algorithms, except that NULL authentication is inapplicable.

2.5. Summary of Changes from RFC 4835

The following is a summary of the changes from RFC 4835.

Old Requirement	New Requirement	Algorithm (notes)
MAY	SHOULD+	AES-GCM with a 16 octet ICV [RFC4106]
MAY	SHOULD+	AES-GMAC with AES-128 [RFC4543]
MUST-	MAY	TripleDES-CBC [RFC2451]
SHOULD NOT	MUST NOT	DES-CBC [RFC2405]
SHOULD+	SHOULD	AES-XCBC-MAC-96 [RFC3566]
SHOULD	MAY	AES-CTR [RFC3686]

3. Usage Guidance

Since ESP and AH can be used in several different ways, this document provides guidance on the best way to utilize these mechanisms.

ESP can provide confidentiality, data origin authentication, or the combination of both of those security services. AH provides only data origin authentication. Background information on those security services is available [RFC4949]. In the following, we shorten "data origin authentication" to "authentication".

Providing both confidentiality and authentication offers the best security. If confidentiality is not needed, providing authentication can still be useful. Confidentiality without authentication is not effective [DP07] and therefore SHOULD NOT be used. We describe each of these cases in more detail below.

To provide both confidentiality and authentication, an authenticated encryption transform from Section 2.1 SHOULD be used in ESP, in conjunction with NULL authentication. Alternatively, an ESP encryption transform and ESP authentication transform MAY be used together. It is NOT RECOMMENDED to use ESP with NULL authentication in conjunction with AH; some configurations of this combination of services have been shown to be insecure [PD10].

To provide authentication without confidentiality, an authentication transform MUST be used in either ESP or AH. The IPsec community generally prefers ESP with NULL encryption over AH. AH is still required in some protocols and operational environments when there are security-sensitive options in the IP header, such as source routing headers; ESP inherently cannot protect those IP options. It is not possible to provide effective confidentiality without authentication, because the lack of authentication undermines the trustworthiness of encryption [B96][V02]. Therefore, an encryption transform MUST NOT be used with a NULL authentication transform (unless the encryption transform is an authenticated encryption transform from Section 2.1).

Triple-DES SHOULD NOT be used in any scenario in which multiple gigabytes of data will be encrypted with a single key. As a 64-bit block cipher, it leaks information about plaintexts above that "birthday bound" [M13]. Triple-DES CBC is listed as a MAY implement for the sake of backwards compatibility, but its use is discouraged.

4. Rationale

This section explains the principles behind the implementation requirements described above.

The algorithms listed as "MAY implement" are not meant to be endorsed over other non-standard alternatives. All of the algorithms that appeared in [RFC4835] are included in this document, for the sake of continuity. In some cases, these algorithms have moved from being "SHOULD implement" to "MAY implement".

4.1. Authenticated Encryption

This document encourages the use of authenticated encryption algorithms because they can provide significant efficiency and throughput advantages, and the tight binding between authentication and encryption can be a security advantage [RFC5116].

AES-GCM [RFC4106] brings significant performance benefits [KKGEGD], has been incorporated into IPsec recommendations [RFC6379], and has emerged as the preferred authenticated encryption method in IPsec and other standards.

4.2. Encryption Transforms

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] [H10].

AES Counter Mode (AES-CTR) is an efficient encryption method, but it provides no authentication capability. The AES-GCM authenticated encryption method has all of the advantages of AES-CTR, while also providing authentication. Thus, this document moves AES-CTR from a SHOULD to a MAY.

The Triple Data Encryption Standard (TDES) is obsolete because of its small block size; as with all 64-bit block ciphers, it SHOULD NOT be used to encrypt more than one gigabyte of data with a single key [M13]. Its key size is smaller than that of the Advanced Encryption Standard (AES), while at the same time its performance and efficiency are worse. Thus, its use in new implementations is discouraged.

The Data Encryption Standard (DES) is obsolete because of its small key size and small block size. There have been publicly demonstrated and open-design special-purpose cracking hardware. Therefore, its use is has been changed to MUST NOT in this document.

4.3. Authentication Transforms

AES-GMAC provides good security along with performance advantages, even over HMAC-MD5. In addition, it uses the same internal components as AES-GCM and is easy to implement in a way that shares components with that authenticated encryption algorithm.

The MD5 hash function has been found to not meet its goal of collision resistance; it is so weak that its use in digital signatures is highly discouraged [RFC6151]. There have been theoretical results against HMAC-MD5, but that message authentication code does not seem to have a practical vulnerability. Thus, it may not be urgent to remove HMAC-MD5 from the existing protocols.

SHA-1 has been found to not meet its goal of collision resistance. However, HMAC-SHA-1 does not rely on this property, and HMAC-SHA-1 is believed to be secure.

HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512 are believed to provide a good security margin, and they perform adequately on many platforms. However, these algorithms are not recommended for implementation in this document, because HMAC-SHA-1 support is widespread and its security is good, AES-GMAC provides good security with better performance, and Authenticated Encryption algorithms do not need any authentication methods.

AES-XCBC has not seen widespread deployment, despite being previously recommended as a SHOULD+ in RFC 4835. Thus, this document lists it only as a SHOULD.

5. Algorithm Diversity

When the AES cipher was first adopted, it was decided to continue encouraging the implementation of Triple-DES, in order to provide algorithm diversity. But the passage of time has eroded the viability of Triple-DES as an alternative to AES. As it is a 64-bit block cipher, its security is inadequate at high data rates (see Section 4.2). Its performance in software and Field-Programmable Gate Arrays (FPGAs) is considerably worse than that of AES. Since it would not be possible to use Triple-DES as an alternative to AES in high data rate environments, or in environments where its performance could not keep up the requirements, the rationale of retaining Triple-DES to provide algorithm diversity is disappearing. (Of course, this does not change the rationale of retaining Triple-DES in IPsec implementations for backwards compatibility.)

Recent discussions in the IETF have started considering how to make the selection of a different cipher that could provide algorithm diversity in IPsec and other IETF standards. That work is expected to take a long time and involve discussions among many participants and organizations.

It is important to bear in mind that it is very unlikely that an exploitable flaw will be found in AES (e.g., a flaw that required less than a terabyte of known plaintext, when AES is used in a conventional mode of operation). The only reason that algorithm diversity deserves any consideration is because there would be large problems if such a flaw were found.

6. Acknowledgements

Some of the wording herein was adapted from [RFC4835], the document that this one obsoletes. That RFC itself borrows from earlier RFCs, notably RFC 4305 and 4307. RFC 4835, RFC 4305, and RFC 4307 were authored by Vishwas Manral, Donald Eastlake, and Jeffrey Schiller respectively.

Thanks are due to Wajdi Feghali, Brian Weis, Cheryl Madson, Dan Harkins, Paul Wouters, Ran Atkinson, Scott Fluhrer, Tero Kivinen, and Valery Smyslov for insightful feedback on this document.

7. Security Considerations

The security of a system that uses cryptography 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 to date leads us to believe that they will likely remain secure into the foreseeable future. However, this is not necessarily forever. Therefore, we expect that revisions of that document will be issued from time to time to reflect the current best practice in this area.

8. References

8.1. Normative References

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

[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.

8.2. Informative References

[B96] Bellovin, S., "Problem areas for the IP security protocols", Proceedings of the Sixth Usenix Unix Security Symposium, 1996.

[DP07] Degabriele, J. and K. Paterson, "Attacking the IPsec Standards in Encryption-only Configurations", IEEE Symposium on Privacy and Security, 2007.

[H10] Hoban, A., "Using Intel AES New Instructions and PCLMULQDQ to Significantly Improve IPSec Performance on Linux", Intel White Paper, August 2010.

[KKGEGD] Kounavis, M., Kang, X., Grewal, K., Eszenyi, M., Gueron, S., and D. Durham, "Encrypting the Internet", SIGCOMM, 2010.

[M13] McGrew, D., "Impossible plaintext cryptanalysis and probable-plaintext collision attacks of 64-bit block cipher modes", IACR ePrint, 2012.

[PD10] Paterson, K. and J. Degabriele, "On the (in)security of IPsec in MAC-then-encrypt configurations", CCS '10, ACM Conference on Computer and Communications Security, 2010.

[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.

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

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

[RFC4835] Manral, V., "Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)", RFC 4835, April 2007.

[RFC4949] Shirey, R., "Internet Security Glossary, Version 2", RFC 4949, August 2007.

[RFC5116] McGrew, D., "An Interface and Algorithms for Authenticated Encryption", RFC 5116, January 2008.

[RFC6151] Turner, S. and L. Chen, "Updated Security Considerations for the MD5 Message-Digest and the HMAC-MD5 Algorithms", RFC 6151, March 2011.

[RFC6379] Law, L. and J. Solinas, "Suite B Cryptographic Suites for IPsec", RFC 6379, October 2011.

[V02] Vaudenay, S., "Security Flaws Induced by CBC Padding - Applications to SSL, IPSEC, WTLS ...", EUROCRYPT, 2002.

Authors' Addresses

David McGrew
Cisco Systems

EMail: mcgrew@cisco.com

Paul Hoffman
VPN Consortium

EMail: paul.hoffman@vpnc.org