Network Working Group
Internet-Draft
Obsoletes: 7321 (if approved)
Intended status: Standards Track
Expires: September 22, 2016

D. Migault
J. Mattsson
Ericsson
P. Wouters
Red Hat
Y. Nir
Check Point

March 21, 2016

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

draft-mglt-ipsecme-rfc7321bis-00

Abstract

This document updates the Cryptographic Algorithm Implementation Requirements for ESP and AH. The goal of these document is to enable ESP and AH to benefit from cryptography that is up to date while making IPsec interoperable.

This document obsoletes RFC 7321 on the cryptographic recommendations only.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on September 22, 2016.

Copyright Notice

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].

This document provides guidance and recommendations so that ESP and AH can be used with a cryptographic algorithms that are up to date. The challenge of such document is to make sure that over the time IPsec implementations can use secure and up-to-date cryptographic algorithms while keeping IPsec interoperable.

Cryptographic algorithms evolves over time...

Sunsetting / introducing new algorithms ...

This document is intended for IPsec developers as well as for IPsec users.

2. 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].

Following [RFC4835], we define some additional key words:

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.

3. ESP Encryption Algorithms

Name	Status	AEAD	Comment
NULL	MUST	No/Yes	[RFC2410]
AES-CBC	MUST-	No	[1] [RFC3602]
AES-GCM with a 16 octet ICV	MUST	Yes	[1] [RFC4106]
CHACHA20_POLY1305	SHOULD	Yes	[RFC7634]
AES-CCM_16	SHOULD	Yes	[1][IoT] [RFC4309]
AES-CCM_8	SHOULD	Yes	[1][IoT] [RFC4309]
3DES	SHOULD NOT	No	[RFC2451]
DES	MUST NOT	No	[RFC2405]

[1] - This requirement level is for 128-bit keys. 256-bit keys are at SHOULD. 192-bit keys can safely be ignored. [IoT] - This requirement is for interoperability with IoT.

IPsec sessions may have very long life time, and carry multiple packets, so there is a need to move 256-bit keys in the long term. For that purpose requirement level is for 128 bit keys and 256 bit keys are at SHOULD (when applicable). In that sense 256 bit keys status has been raised from MAY in RFC7321 to SHOULD.

NULL status remains to MUST to enable the use of ESP with only authentication. It status is expected to remain MUST by protocol requirements.

ENCR_AES_CBC status remains to MUST in order to enable interoperability between implementation that followed RFC7321.

AES-GCM status has been updated from SHOULD+ to MUST in order to favor the use of authenticated encryption and AEAD algorithms. The main motivation for adopting AES-GCM for ESP is performance as well as key longevity - compared to AES-CBC for example. This resulted in AES-GCM widely implemented for ESP.

ENCR_CHACHA20_POLY1305 was not ready to be considered at the time of RFC7321. It has been recommended by the CRFG and others as an alternative to AES and AES-GCM. It is also being standardized for IPsec for the same reasons. At the time of writing, there were not enough ESP implementations of ENCR_CHACHA20_POLY1305 to be able to introduce it at the SHOULD+ level.

ENCR_AES_CCM_8-16 status have been raised from MAY to SHOULD. This document considers it SHOULD be implemented in order to be able to interact with Internet of Things devices. As this case is not a general use case for VPNs, its status is expected to remain to SHOULD.

ENCR_3DES status has been downgraded from MAY in RFC7321 to SHOULD NOT. However, ENCR_CHACHA20_POLY1305 seems a more modern approach alternative to AES than 3DES and so it expected to be favored over

3DES.

ENCR_DES status remains to MUST NOT.

4. ESP and AH Authentication Algorithms

Encryption without authentication MUST NOT be used. As a result, authentication algorithm recommendations in this section are targeting two types of communications: Firstly authenticated only communications without encryption -- such communications can be ESP with NULL encryption or AH communications. Secondly, communications that are encrypted with non AEAD encryption algorithms mentioned above. In this case, they MUST be combined with an authentication algorithm.

Name	Status	Comment
AES-128-GMAC	MUST	[RFC4553]
AES-256-GMAC	SHOULD	[RFC4553]
HMAC_SHA2_256_128	SHOULD	[RFC4868]
HMAC_SHA2_512_256	SHOULD	[RFC4868]
HMAC_SHA1_96	MUST-	[RFC2404]
AES_XCBC_96	SHOULD	[IoT] [RFC3566]
NULL	MUST NOT	only acceptable for authenticated encryption [RFC4303]

[IoT] - This requirement is for interoperability with IoT

HMAC_SHA2_256_128 was not mentioned in RFC7321, as no SHA2 based

authentication was mentioned. HMAC_SHA2_256_128 SHOULD be implemented in order to replace HMAC_SHA1_96.

HMAC_SHA2_512_256 SHOULD be implemented as a future replacement of HMAC_SHA2_256_128 or when stronger security is required. This value has been preferred to HMAC_SHA2_384, as the overhead of HMAC_SHA2_512 is negligible.

HMAC_SHA1_96 status has been downgraded from MUST in RFC7321 to MUST- as there is an industry-wide trend to deprecate its usage.

AES-XCBC is only recommended in the scope of IoT, as Internet of Things deployments tend to prefer AES based HMAC functions in order to avoid implementing SHA2. For the wide VPN deployment, as it has not been widely adopted, it has been downgraded from SHOULD in RFC4307 to MAY.

AES-128-GMAC status is being upgraded from SHOULD+ to MUST in order to guarantee interoperability between implementation that are following RFC7321 and this document. In fact HMAC-SHA1-96 was used to be the algorithm that provided interoperability and it has been downgraded.

AES-256-GMAC was not mentioned in RFC7321. Its status has been set to SHOULD as as a future replacement of AES-128-GMAC or when stronger security is required.

NULL has been downgraded from MAY in RFC7321 to MUST NOT. The only reason NULL is acceptable is when authenticated encryption algorithms are selected from Section 3. In any other case, NULL MUST NOT be selected. As ESP and AH provides both authentication, one may be tempted to combine these protocol to provide authentication. As mentionned by RFC7321, it is NOT RECOMMENDED to use ESP with NULL authentication - with non authenticated encryption - in conjunction with AH; some configurations of this combination of services have been shown to be insecure [PD10]. In addition, ESP NULL authentication cannot be combined with ESP NULL encryption.

5. Summary of Changes from RFC 7321

I think that would be interesting to document and summarize the changes.

6. Acknowledgements

7. IANA Considerations

None.

8. Security Considerations

9. References

9.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <http://www.rfc-editor.org/info/rfc2119>.

[RFC4301] Kent, S. and K. Seo, "Security Architecture for the Internet Protocol", RFC 4301, DOI 10.17487/RFC4301, December 2005, <http://www.rfc-editor.org/info/rfc4301>.

[RFC4302] Kent, S., "IP Authentication Header", RFC 4302, DOI 10.17487/RFC4302, December 2005, <http://www.rfc-editor.org/info/rfc4302>.

[RFC4303] Kent, S., "IP Encapsulating Security Payload (ESP)", RFC 4303, DOI 10.17487/RFC4303, December 2005, <http://www.rfc-editor.org/info/rfc4303>.

[RFC7321] McGrew, D. and P. Hoffman, "Cryptographic Algorithm Implementation Requirements and Usage Guidance for Encapsulating Security Payload (ESP) and Authentication Header (AH)", RFC 7321, DOI 10.17487/RFC7321, August 2014, <http://www.rfc-editor.org/info/rfc7321>.

[RFC7634] Nir, Y., "ChaCha20, Poly1305, and Their Use in the Internet Key Exchange Protocol (IKE) and IPsec", RFC 7634,

DOI 10.17487/RFC7634, August 2015,
<http://www.rfc-editor.org/info/rfc7634>.

9.2. Informative References

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

[RFC2404] Madson, C. and R. Glenn, "The Use of HMAC-SHA-1-96 within ESP and AH", RFC 2404, DOI 10.17487/RFC2404, November 1998, <http://www.rfc-editor.org/info/rfc2404>.

[RFC2405] Madson, C. and N. Doraswamy, "The ESP DES-CBC Cipher Algorithm With Explicit IV", RFC 2405, DOI 10.17487/RFC2405, November 1998, <http://www.rfc-editor.org/info/rfc2405>.

[RFC2410] Glenn, R. and S. Kent, "The NULL Encryption Algorithm and Its Use With IPsec", RFC 2410, DOI 10.17487/RFC2410, November 1998, <http://www.rfc-editor.org/info/rfc2410>.

[RFC2451] Pereira, R. and R. Adams, "The ESP CBC-Mode Cipher Algorithms", RFC 2451, DOI 10.17487/RFC2451, November 1998, <http://www.rfc-editor.org/info/rfc2451>.

[RFC3566] Frankel, S. and H. Herbert, "The AES-XCBC-MAC-96 Algorithm and Its Use With IPsec", RFC 3566, DOI 10.17487/RFC3566, September 2003, <http://www.rfc-editor.org/info/rfc3566>.

[RFC3602] Frankel, S., Glenn, R., and S. Kelly, "The AES-CBC Cipher Algorithm and Its Use with IPsec", RFC 3602, DOI 10.17487/RFC3602, September 2003, <http://www.rfc-editor.org/info/rfc3602>.

[RFC3686] Housley, R., "Using Advanced Encryption Standard (AES) Counter Mode With IPsec Encapsulating Security Payload (ESP)", RFC 3686, DOI 10.17487/RFC3686, January 2004, <http://www.rfc-editor.org/info/rfc3686>.

[RFC4106] Viega, J. and D. McGrew, "The Use of Galois/Counter Mode

(GCM) in IPsec Encapsulating Security Payload (ESP)", RFC 4106, DOI 10.17487/RFC4106, June 2005, <http://www.rfc-editor.org/info/rfc4106>.

[RFC4309] Housley, R., "Using Advanced Encryption Standard (AES) CCM Mode with IPsec Encapsulating Security Payload (ESP)", RFC 4309, DOI 10.17487/RFC4309, December 2005, <http://www.rfc-editor.org/info/rfc4309>.

[RFC4543] McGrew, D. and J. Viega, "The Use of Galois Message Authentication Code (GMAC) in IPsec ESP and AH", RFC 4543, DOI 10.17487/RFC4543, May 2006, <http://www.rfc-editor.org/info/rfc4543>.

[RFC4835] Manral, V., "Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)", RFC 4835, DOI 10.17487/RFC4835, April 2007, <http://www.rfc-editor.org/info/rfc4835>.

Authors' Addresses

Daniel Migault
Ericsson
8400 boulevard Decarie
Montreal, QC H4P 2N2
Canada

Phone: +1 514-452-2160
Email: daniel.migault@ericsson.com

John Mattsson
Ericsson AB
SE-164 80 Stockholm
Sweden

Email: john.mattsson@ericsson.com

Paul Wouters
Red Hat

Email: pwouters@redhat.com

Yoav Nir
Check Point Software Technologies Ltd.
5 Hasolelim st.
Tel Aviv 6789735
Israel

Email: ynir.ietf@gmail.com