Groupe de travail Réseau
Request for Comments : 4835
RFC rendue obsolète : 4305
Catégorie : En cours de normalisation

V. Manral, IP Infusion Inc.
avril 2007

Traduction Claude Brière de L'Isle

Exigences de mise en œuvre d'algorithme cryptographique pour l'encapsulation de charge utile de sécurité (ESP) et l'en-tête d'authentification (AH)

Statut du présent mémoire
Le présent document spécifie un protocole en cours de normalisation de l'Internet pour la communauté de l'Internet, et appelle à des discussion et suggestions pour son amélioration. Prière de se référer à l'édition en cours des "Normes officielles des protocoles de l'Internet" (STD 1) pour connaître l'état de la normalisation et le statut de ce protocole. La distribution du présent mémoire n'est soumise à aucune restriction.

Notice de Copyright
Copyright (C) The IETF Trust (2007).

Résumé

La série des protocoles IPsec utilise divers algorithmes cryptographiques afin d'assurer des services de sécurité. L'encapsulation de charge utile de sécurité (ESP, *Encapsulating Security Payload*) et l'en-tête d'authentification (AZ, *Authentication Header*) fournissent deux mécanismes pour protéger les données qui sont envoyées sur une association de sécurité (SA, *Security Association*) IPsec. Pour assurer l'interopérabilité entre des mises en œuvre disparates, il est nécessaire de spécifier un ensemble d'algorithmes de mise en œuvre obligatoire pour garantir qu'il y a au moins un algorithme qui sera disponible pour toutes les mises en œuvre. Le présent document définit l'ensemble actuel des algorithmes de mise en œuvre obligatoire pour ESP et AH et spécifie aussi les algorithmes qui devraient être mis en œuvre parce qu'ils pourraient être promus au rang des obligatoires à l'avenir.

Table des matières

1. Introduction

L'encapsulation de charge utile de sécurité (ESP, *Encapsulating Security Payload*) et l'en-tête d'authentification (AH, *Authentication Header*) fournissent deux mécanismes pour protéger les données envoyées sur une association de sécurité (SA, *Security Association*) IPsec [RFC4301], [RFC4302]. Pour assurer l'interopérabilité entre des mises en œuvre disparates, il est nécessaire de spécifier un ensemble d'algorithmes de mise en œuvre obligatoire pour garantir qu'il y a au moins un algorithme qui sera disponible pour toutes les mises en œuvre. Le présent document définit l'ensemble actuel d'algorithmes de mise en œuvre obligatoire pour ESP et AH ainsi qu'il spécifie les algorithmes qui devraient être mis en œuvre parce qu'ils pourraient être promus au rang des obligatoires à l'avenir.

La nature de la cryptographie est telle que de nouveaux algorithmes apparaissent continuellement et que les algorithmes existants sont continuellement attaqués. Un algorithme tenu pour fort aujourd'hui peut voir sa faiblesse démontrée demain. Cela étant, le choix d'algorithmes de mise en œuvre obligatoire devrait être prudent de façon à minimiser la probabilité qu'il soit rapidement compromis. On devrait aussi penser aux considérations de performances car de nombreuses utilisations de IPsec seront dans des environnements où est présent le souci des performances.

Finalement, on doit reconnaître que les algorithmes de mise en œuvre obligatoire peuvent avoir besoin de changer avec le temps pour s'adapter aux changements du monde. Pour cette raison, le choix des algorithmes de mise en œuvre obligatoire n'est pas inclus dans les principales spécifications d'IPsec, ESP, ou AH. À la place, il est placé dans le présent document. Comme le choix d'algorithme change, seul ce document aura besoin d'être mis à jour.

Idéalement, l'algorithme de mise en œuvre obligatoire de demain devrait être déjà être disponible dans la plupart des mises en œuvre de IPsec au moment où il devient obligatoire. Pour faciliter cela, on va tenter d'identifier de tels algorithmes (car ils sont aujourd'hui connus) dans le présent document. Il n'est pas garanti que les algorithmes dont on croit (aujourd'hui) qu'ils pourraient être obligatoires à l'avenir le deviendront bien. Tous les algorithmes connus aujourd'hui sont sujets à des attaques cryptographiques et pourraient être cassés à l'avenir.

2. Terminologie des exigences

Dans le présent document, les mots clés "DOIT", "NE DOIT PAS", "EXIGE", "DEVRA", "NE DEVRA PAS", "DEVRAIT", "NE DEVRAIT PAS", "RECOMMANDE", "PEUT", et "FACULTATIF" sont à interpréter comme décrit dans la [RFC 2119].

On définit ici des termes supplémentaires :

DEVRAIT+ : ce terme signifie la même chose que DEVRAIT. Cependant, il est probable qu'un algorithme marqué DEVRAIT+ sera promu à l'avenir pour devenir un DOIT.

DEVRAIT- : de terme signifie la même chose que DEVRAIT. Cependant, il est probable qu'un algorithme marqué DEVRAIT- sera dégradé en un PEUT ou pire dans une future version de ce document.

DOIT- : ce terme signifie la même chose que DOIT. Cependant, on s'attend qu'à l'avenir, cet algorithme ne soit plus un DOIT.

3. Choix d'algorithme

Pour que les mises en œuvre d'IPsec interopèrent, elles doivent prendre en charge en commun un ou plusieurs algorithmes de sécurité. La présente section spécifie les exigences de mise en œuvre d'algorithmes de sécurité pour les mises en œuvre d'ESP et AH conformes aux normes. Les algorithmes de sécurité actuellement utilisés pour toute association de sécurité ESP ou AH particulière sont déterminés par un mécanisme de négociation, comme dans l'échange de clé Internet (IKE, *Internet Key Exchange*) [RFC2409], [RFC4306] ou par pré établissement.

Bien sûr, des algorithmes standard et brevetés au delà de ceux énumérés ci-dessous peuvent être mis en œuvre.

3.1 Encapsulation de charge utile de sécurité

Les exigences de conformité de mise en œuvre pour les algorithmes de sécurité pour ESP sont données dans les tableaux ci-dessous. Voir à la Section 2 les définitions des valeurs dans la colonne "Exigence".

3.1.1 Algorithmes de chiffrement et d'authentification d'ESP

Ces tableaux énumèrent les algorithmes de chiffrement et d'authentification pour le protocole d'encapsulation de charge utile de sécurité IPsec .

Exigence	**Algorithme de chiffrement** (notes)
DOIT	NULL [RFC2410] (1)
DOIT	AES-CBC avec clé de 128 bits [RFC3602]
DOIT-	TripleDES-CBC [RFC2451]
DEVRAIT	AES-CTR [RFC3686]
NE DEVRAIT PAS	DES-CBC [RFC2405] (2)

Exigence	**Algorithme de d'authentification** (notes)
DOIT	HMAC-SHA1-96 [RFC2404] (3)
DEVRAIT+	AES-XCBC-MAC-96 [RFC3566]
PEUT	NULL (1)
PEUT	HMAC-MD5-96 [RFC2403] (4)

Notes :
(1) Comme le chiffrement ESP est facultatif; la prise en charge de l'algorithme "NULL" est exigée pour garder la cohérence avec la façon dont les services sont négociés. Noter qu'alors que l'authentification et le chiffrement peuvent chacun être "NULL", ils NE DOIVENT PAS être tous deux "NULL" [RFC4301].
(2) DES, avec sa petite taille de clé et un matériel spécialement conçu pour le craquer d'accès libre et publiquement démontré est d'une sécurité questionnable pour une utilisation générale.
(3) Des faiblesses sont devenues apparentes dans SHA-1 [SHA1-COLL] ; cependant, elles ne devraient pas affecter l'utilisation de SHA1 avec HMAC.
(4) Des faiblesses sont devenues apparentes dans MD5 [MD5-COLL] ; cependant, elles ne devraient pas affecter l'utilisation de MD5 avec HMAC.

3.1.2 Algorithmes d'ESP en mode combiné

Comme spécifié dans la [RFC4303], des algorithmes en mode combiné sont pris en charge pour fournir des services à la fois de confidentialité et d'authentification. La prise en charge de tels algorithmes exigera une structuration appropriée des mises en œuvre d'ESP. Dans de nombreuses circonstances, les algorithmes en mode combiné fournissent une efficacité significative et des avantages en débit. Bien qu'il n'y ait pas d'algorithme combiné suggéré ou exigé à l'heure actuelle, AES-CCM [RFC4309] et AES-GCM [RFC4106] sont dignes d'intérêt. AES-CCM a été adopté comme mode préféré dans la norme IEEE 802.11 [802.11i], et AES-GCM a été adopté comme mode préféré dans la norme IEEE 802.1ae [802.1ae].

3.2 En-tête d'authentification

Les exigences de conformité de mise en œuvre pour les algorithmes de sécurité pour AH sont données ci-dessous. Voir à la Section 2 la définition des valeurs dans la colonne "Exigence". Comme on s'en doute, tous ces algorithmes sont des algorithmes d'authentification.

Exigence	**Algorithme** (notes)
DOIT	HMAC-SHA1-96 [RFC2404] (1)
DEVRAIT+	AES-XCBC-MAC-96 [RFC3566]
PEUT	HMAC-MD5-96 [RFC2403] (2)

Notes :
(1) Des faiblesses sont devenues apparentes dans SHA-1 [SHA1-COLL] ; cependant, elles ne devraient pas affecter l'utilisation de SHA1 avec HMAC.
(2) Des faiblesses sont devenues apparentes dans MD5 [MD5-COLL] ; cependant, elles ne devraient pas affecter l'utilisation de MD5 avec HMAC.

4. Considérations pour la sécurité

La sécurité des systèmes fondés sur la cryptographie dépend à la fois de la force des algorithmes cryptographiques choisis et de la force des clés utilisées avec ces algorithmes. La sécurité dépend aussi de l'ingénierie et de l'administration du protocole utilisé par le système pour assurer qu'il n'y a pas de façon non cryptographique de subvertir la sécurité du système global.

Le présent document concerne le choix des algorithmes cryptographiques pour l'utilisation de ESP et AH, en particulier avec le choix d'algorithmes de mise en œuvre obligatoire. Les algorithmes identifiés dans le présent document par "DOIT mettre en œuvre" ou "DEVRAIT mettre en œuvre" ne sont pas réputés cassables pour l'instant, et les recherches en cryptographie menées jusqu'à présent laissent penser qu'ils resteront sûrs dans l'avenir prévisible. Cependant, cela ne veut pas nécessairement dire pour toujours. On s'attend donc à ce que de nouvelles révisions de ce document soient publiées de temps en temps pour refléter les bonnes pratiques en cours dans ce domaine.

5. Remerciements

Beaucoup du texte de ce document a été adapté de la RFC4305, le document père du présent document. La RFC4305 elle-même empruntait le texte de la [RFC4307], "Algorithmes cryptographiques à utiliser avec la version 2 de l'échange de clés sur Internet (IKEv2)", par Jeffrey I. Schiller.

Merci aux personnes suivantes pour leurs rapports ou leur réponse aux rapports sur les erreurs de la RFC4305 : Paul Hoffman, Stephen Kent, Paul Koning, et Lars Volker. Des commentaires utiles sur le dernier appel ont été reçus de Russ Housley, Elwyn Davies, Nicolas Williams, et Alfred Hoenes.

6. Changements de la RFC 2402 et de la RFC 2406 à la RFC 4305

La [RFC2402] et la [RFC2406] définissaient l'en-tête d'authentification IPsec et l'encapsulation de charge utile de sécurité IPsec. Chacune spécifiait les exigences de mise en œuvre des algorithmes de chiffrement pour leur protocoles respectifs. Elles ont maintenant été remplacées par les [RFC4302] et [RFC4303], qui ne spécifient pas d'exigences de mise en œuvre d'algorithme cryptographique, et par le présent document, qui spécifie de telles exigences pour les deux [RFC4302] et [RFC4303].

Les exigences de mise en œuvre sont comparées ci-dessous :

Ancienne exigence	**Ancienne RFC**	**Nouvelle exigence**	**Algorithme**
DOIT	2406	NE DEVRAIT PAS	DES-CBC [RFC2405] (note)
DOIT	2402 2406	PEUT	HMAC-MD5-96 [RFC2403]
DOIT	2402 2406	DOIT	HMAC-SHA1-96 [RFC2404]

Note : L'IETF a déconseillé depuis des années l'utilisation de DES seul et ne l'a pas inclus depuis un certain temps dans les nouvelles normes (voir la note de l'IESG à la première page de la [RFC2407]). La [RFC4305] a représenté la première reconnaissance de ce conseil dans un document en cours de normalisation en spécifiant que les mises en œuvre NE DEVRAIENT PAS fournir DES seul. L'Institut national des normes et technologies (NIST) du Gouvernement américain a formellement reconnu la faiblesse de DES seul par une note publiée [DES-WDRAW] proposant de le retirer comme norme du gouvernement US. Triple DES reste approuvé à la fois par l'IETF et le NIST.

7. Changements depuis la RFC 4305

Le présent document rend obsolète la [RFC4305]. Il incorpore les changements pour la prise en charge de l'algorithme d'authentification NUL en transformant la prise en charge de DOIT en PEUT. Ce changement est fait pour assurer la cohérence avec la [RFC4301]. on a ajouté un texte sur les attaques de collision contre SHA-1 ainsi que sur l'utilisation future de AES-GCM et de AES-CCM.

Les changements d'exigence de mise en œuvre résultant de ces modifications sont énumérés ci-dessous :

Ancienne exigence	**Vieille RFC**	**Nouvelle exigence**	**Nouvel algorithme** (notes)
DOIT	2406	PEUT	Authentification NULLE
DOIT	2406	DOIT	Chiffrement NUL
DEVRAIT	4305	DOIT	Chiffrement AES-CBC

8. Références

8.1 Références normatives

[RFC2119] S. Bradner, "Mots clés à utiliser dans les RFC pour indiquer les niveaux d'exigence", BCP 14, mars 1997.

[RFC2403] C. Madson, R. Glenn, "Utilisation de HMAC-MD5-96 au sein d'ESP et d'AH", novembre 1998. *(P.S.)*

[RFC2404] C. Madson, R. Glenn, "Utilisation de HMAC-SHA-1-96 au sein d'ESP et d'AH", novembre 1998. *(P.S.)*

[RFC2405] C. Madson et N. Doraswamy, "Algorithme de chiffrement ESP DES-CBC avec IV explicite", novembre 1998.

[RFC2410] R. Glenn, S. Kent, "L'algorithme de chiffrement NULL et son utilisation avec IPsec", novembre 1998. *(P.S.)*

[RFC2451] R. Pereira, R. Adams, "Algorithmes de chiffrement ESP en mode CBC", novembre 1998. *(P.S.)*

[RFC3566] S. Frankel, H. Herbert, "L'algorithme AES-XCBC-MAC-96 et son utilisation avec IPsec", septembre 2003. *(P.S.)*

[RFC3602] S. Frankel, R. Glenn, S. Kelly, "Algorithme de chiffrement AES-CBC et utilisation avec IPsec", septembre 2003.

[RFC3686] R. Housley, "Utilisation du mode Compteur de la norme de chiffrement évolué (AES) avec l'encapsulation de

la charge utile de sécurité (ESP) dans IPsec", janvier 2004. *(P.S.)*

[RFC4301] S. Kent et K. Seo, "Architecture de sécurité pour le protocole Internet", décembre 2005. *(P.S.)*

[RFC4302] S. Kent, "En-tête d'authentification IP", décembre 2005. *(P.S.)*

[RFC4303] S. Kent, "Encapsulation de charge utile de sécurité dans IP (ESP)", décembre 2005. (Remplace RFC2406) *(P.S.)*

[RFC4305] D. Eastlake 3rd, "Exigences de mise en œuvre d'algorithme cryptographique pour l'encapsulation de charge utile de sécurité (ESP) et l'en-tête d'authentification (AH)", décembre 2005. *(P.S.)* (*Obsolète, voir* RFC4835)

8.2 Références pour information

[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, juin 2004.

[802.1ae] "Media Access Control (MAC) Security", IEEE Standard Medium Access Control (MAC) Security, IEEE Std 802.1ae, juin 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, juillet 2004.

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

[RFC2402] S. Kent et R. Atkinson, "En-tête d'authentification IP", novembre 1998. (*Obsolète, voir* RFC4302, 4305)

[RFC2406] S. Kent et R. Atkinson, "Encapsulation de charge utile de sécurité IP (ESP)", novembre 1998. *(Obsolète, voir RFC 4303)*

[RFC2407] D. Piper, "Le domaine d'interprétation de sécurité IP de l'Internet pour ISAKMP", novembre 1998. *(Obsolète, voir 4306)*

[RFC2409] D. Harkins et D. Carrel, "L'échange de clés Internet (IKE)", novembre 1998. *(Obsolète, voir la RFC 4306)*

[RFC4106] J. Viega, D. McGrew, "Utilisation du mode Galois/Compteur (GCM) dans une charge utile de sécurité par encapsulation (ESP) IPsec", juin 2005. *(P.S.)*

[RFC4306] C. Kaufman, "Protocole d'échange de clés sur Internet (IKEv2)", décembre 2005.

[RFC4307] J. Schiller, "Algorithmes cryptographiques à utiliser avec la version 2 de l'échange de clés sur Internet (IKEv2)", décembre 2005. *(P.S.)*

[RFC4309] R. Housley, "Utilisation du mode CCM de la norme de chiffrement évolué (AES) avec l'encapsulation de charge utile de sécurité (ESP) dans IPsec", décembre 2005. *(P.S.)*

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

Adresse de l'auteur

Vishwas Manral
IP Infusion Inc.
Bamankhola, Bansgali,
Almora, Uttarakhand 263601
India
téléphone : +91-98456-61911
mél : vishwas@ipinfusion.com

Déclaration de droits de reproduction

Copyright (C) The IETF Trust (2007).

Le présent document est soumis aux droits, licences et restrictions contenus dans le BCP 78, et à www.rfc-editor.org, et sauf pour ce qui est mentionné ci-après, les auteurs conservent tous leurs droits.

Le présent document et les informations qui y sont contenues sont fournis sur une base "EN L'ÉTAT" et le contributeur, l'organisation qu'il ou elle représente ou qui le/la finance (s'il en est), la INTERNET SOCIETY et la INTERNET ENGINEERING TASK FORCE déclinent toutes garanties, exprimées ou implicites, y compris mais non limitées à toute garantie que l'utilisation des informations ci encloses ne violent aucun droit ou aucune garantie implicite de commercialisation ou d'aptitude à un objet particulier.

Propriété intellectuelle

L'IETF ne prend pas position sur la validité et la portée de tout droit de propriété intellectuelle ou autres droits qui pourraient être revendiqués au titre de la mise en œuvre ou l'utilisation de la technologie décrite dans le présent document ou sur la mesure dans laquelle toute licence sur de tels droits pourrait être ou n'être pas disponible ; pas plus qu'elle ne prétend avoir accompli aucun effort pour identifier de tels droits. Les informations sur les procédures de l'ISOC au sujet des droits dans les documents de l'ISOC figurent dans les BCP 78 et BCP 79.

Des copies des dépôts d'IPR faits au secrétariat de l'IETF et toutes assurances de disponibilité de licences, ou le résultat de tentatives faites pour obtenir une licence ou permission générale d'utilisation de tels droits de propriété par ceux qui mettent en œuvre ou utilisent la présente spécification peuvent être obtenues sur le répertoire en ligne des IPR de l'IETF à http://www.ietf.org/ipr.

L'IETF invite toute partie intéressée à porter son attention sur tous copyrights, licences ou applications de licence, ou autres droits de propriété qui pourraient couvrir les technologies qui peuvent être nécessaires pour mettre en œuvre la présente norme. Prière d'adresser les informations à l'IETF à ietf- ipr@ietf.org.

Remerciement

Le financement de la fonction d'édition des RFC est actuellement fourni par la Internet Society.