Internet Engineering Task Force (IETF)
Request for Comments : 7146
RFC mises à jour : 3720, 3723, 3821, 3822, 4018, 4172, 4173, 4174, 5040, 5041, 5042, 5043, 5044, 5045, 5046, 5047, 5048
Catégorie : Sur la voie de la normalisation
ISSN : 2070-1721

D. Black, EMC
P. Koning, Dell

avril 2014
Traduction Claude Brière de L'Isle

Sécurisation des protocoles de mémorisation de bloc sur IP : mise à jour des exigences de la RFC 3723 pour IPsec v3

Résumé
La RFC 3723 spécifie les exigences d'IPsec pour les protocoles de mémorisation de blocs sur IP (par exemple, l'interface Internet de système de petit ordinateur (iSCSI, *Internet Small Computer System Interface*)) sur la base de IPsec v2 ([RFC2401] et les RFC qui s'y rapportent) ; ces exigences ont ensuite été appliquées aux protocoles de placement direct de données à distance, par exemple, le protocole d'accès direct à une mémoire distante (RDMAP, *Remote Direct Memory Access Protocol*). Le présent document met à jour les exigences IPsec de la RFC 3723 avec IPsec v3 ([RFC4301] et les RFC qui s'y rapportent) et apporte des changements aux algorithmes exigés sur la base des développements en cryptographie depuis la publication de la RFC 3723.

Table des matières

1. Introduction

La [RFC3723] spécifie les exigences IPsec pour les protocoles de mémorisation de bloc sur IP (par exemple, iSCSI [RFC3720]) fondés sur IPsec v2 ([RFC2401] et les RFC qui s'y rapportent) ; ces exigences ont ensuite été appliquées aux protocoles de placement direct de données à distance, par exemple, RDMAP [RFC5040]. Le présent document met à jour les exigences IPsec de la RFC 3723 avec IPsec v3 ([RFC4301] et les RFC qui s'y rapportent) pour refléter les développements depuis la publication de la RFC 3723.

En bref, le présent document utilise le terme de "protocoles de mémorisation de bloc" pour se référer à tous les protocoles auxquels s'appliquent les exigences de la RFC 3723 ; voir les détails au paragraphe 1.3.

En plus des exigences de IPsec v2 de la RFC 3723, IPsec v3, tel que spécifié dans la [RFC4301] et les RFC qui s'y rapportent (par exemple, IKEv2 [RFC5996]), DEVRAIT être mis en œuvre pour les protocoles de mémorisation de bloc. La conservation des exigences obligatoires de IPsec v2 assure l'interopérabilité avec les les mises en œuvre existantes, et la forte recommandation de IPsec v3 encourage les mises en œuvre à passer à cette plus récente version de IPsec.

Les développements de la cryptographié depuis la publication de la RFC 3723 nécessitent des changements aux exigences de transformations de chiffrement pour IPsec v2, comme c'est expliqué au paragraphe 2.2 ; ces exigences mises à jour s'appliquent aussi à IPsec v3.

Les protocoles de mémorisation de bloc peuvent fonctionner à de hauts débits de données (plusieurs gigabits/s). Les exigences cryptographiques du présent document sont fortement influencées par ce fait ; un important exemple est que le chaînage de bloc de chiffrement de la norme de triple chiffrement de données (3DES CBC, *Triple Data Encryption Standard Cipher Block Chaining*) n'est plus recommandé pour les protocoles de mémorisation de bloc à cause de l'impact des fréquents changements de clés de la taille de bloc de 64 bits de 3DES aux hauts débits de données.

1.1 Langage des exigences

Les mots clés "DOIT", "NE DOIT PAS", "EXIGE", "DEVRA", "NE DEVRA PAS", "DEVRAIT", "NE DEVRAIT PAS", "RECOMMANDE", "PEUT", et "FACULTATIF" dans ce document sont à interpréter comme décrit dans la [RFC2119].

1.2 Résumé des changements à la RFC 3723

Le présent document apporte les changements suivants à la RFC 3723 :

- Ajoute l'exigence que IPsec v3 DEVRAIT être mis en œuvre (Encapsulation de charge utile de sécurité (ESPv3) et IKEv2) en plus de IPsec v2 (voir la Section 1).
- Exige les numéros de séquence étendus pour ESPv2 et ESPv3 (voir la Section 2).
- Précise les exigences de taille de clé pour MAC CBC AES avec les extensions XCBC (DOIT mettre en œuvre des clés de 128 bits ; voir le paragraphe 2.1).
- Ajoute les exigences de IPsec v3 pour le code d'authentification de message de Galois AES (GMAC) et le mode Galois/compteur (GCM) (DEVRAIT mettre en œuvre quand IKEv2 est pris en charge ; voir les paragraphes 2.1 et 2.2).
- Supprime les exigences de mise en œuvre de CBC 3DES et d'AES en mode Compteur (AES CTR) (change les exigences pour les deux en "PEUT mettre en œuvre"). Ajoute l'exigence de "DOIT mettre en œuvre" pour AES CBC (voir au paragraphe 2.2).
- Ajoute les exigences de mise en œuvre spécifiques de IKEv2 (voir la Section 3).
- Supprime l'exigence que IKEv1 utilise l'accès UDP 500 (voir la Section 3).
- Permet l'utilisation du protocole d'état de certificat en ligne (OSCP, *Online Certificate Status Protocol*) en plus des listes de révocation de certificats (CRL, *Certificate Revocation List*) pour vérifier les certificats, et change la recommandation de taille de groupe Diffie-Hellman à un minimum de 2048 bits (voir la Section 3).

1.3 Autres RFC mises à jour

Les exigences IPsec de la RFC 3723 ont été appliquées à un certain nombre de protocoles. Pour cette raison, en plus de la mise à jour des exigences IPsec de la RFC 3723, le présent document met aussi à jour les exigences IPsec pour chaque protocole qui utilise la RFC 3723 ; c'est-à-dire que les RFC suivantes sont mises à jour -- dans chaque cas, la mise à jour porte seulement sur les exigences IPsec :

- [RFC3720] "Interface Internet de petites systèmes d'ordinateur (iSCSI)"

- [RFC3821] "Canal fibre sur TCP/IP (FCIP)"
- [RFC3822] "Découverte de canal fibre sur des entités TCP/IP (FCIP) en utilisant le protocole de localisation de service version 2 (SLPv2)"
- [RFC4018] "Découverte de cibles et des serveurs de noms des interfaces Internet de systèmes de petits ordinateurs (iSCSI) en utilisant le protocole de localisation de service version 2 (SLPv2)"
- [RFC4172] "iFCP – un protocole pour le réseautage des mises en mémoire de canal fibre sur Internet"
- [RFC4173] "Clients d'amorçage qui utilisent le protocole d'interface Internet de système de petit ordinateur (iSCSI)"
- [RFC4174] "Option IPv4 du protocole de configuration dynamique d'hôte (DHCP) pour le service de noms de mémorisation sur Internet"
- [RFC5040] "Spécification d'un protocole d'accès direct à une mémoire distante"
- [RFC5041] "Placement direct des données sur transports fiables"
- [RFC5042] "Sécurité du protocole de placement direct des données (DDP) / protocole d'accès direct à une mémoire distante (RDMAP)"
- [RFC5043] "Adaptation du placement direct des données (DDP) au protocole de transmission de contrôle de flux (SCTP)"
- [RFC5044] "Tramage verrouillé sur la PDU de marqueur pour la spécification de TCP"
- [RFC5045] "Applicabilité du protocole d'accès direct à une mémoire distante (RDMA) et du placement direct des données (DDP)"
- [RFC5046] "Extensions pour l'accès direct à une mémoire distante (RDMA) à l'interface Internet de système de petit ordinateur (iSCSI)"
- [RFC5047] "DA : Architecture Datamover pour l'interface Internet de système de petit ordinateur (iSCSI)"
- [RFC5048] "Corrections et précisions à l'interface Internet de système de petit ordinateur (iSCSI)"

Les [RFC3721] et [RFC5387] ne sont pas mises à jour par le présent document, car leur utilisation de la RFC 3723 n'englobe pas ses exigences IPsec.

De plus, la mise à jour des exigences IPsec du présent document s'applique aux nouvelles spécifications pour iSCSI [RFC7143] et aux extensions iSCSI pour RDMA (iSER) [RFC7145].

Le présent document utilise le terme de "protocole de mémorisation de bloc" pour se référer aux protocoles (mentionnés ci-dessus) auxquels s'appliquent les exigences de la RFC 3723 (telle que mise à jour par les exigences du présent document).

2. Exigences pour ESP

La RFC 3723 exige que les mises en œuvre DOIVENT prendre en charge IPsec ESPv2 [RFC2406] en mode tunnel au titre de IPsec v2 pour fournir la sécurité à la fois pour les paquets de contrôle et les paquets de données, et que quand ESPv2 est utilisé, l'authentification de l'origine des données par paquet, la protection de l'intégrité et contre la répétition DOIT être fournie.

Le présent document modifie la RFC 3723 pour exiger que les mises en œuvre DEVRAIENT aussi prendre en charge IPsec ESPv3 [RFC4303] en mode tunnel au titre de IPsec v3 pour fournir la sécurité aussi bien des paquets de contrôle que des paquets de données, l'authentification de l'origine des données par paquet, la protection de l'intégrité, et contre la répétition DOIT être fournie quand ESPv3 est utilisé.

Aux grandes vitesses auxquelles les protocoles de mémorisation de bloc sont supposés fonctionner, une seule association de sécurité IPsec (SA) pourrait rapidement épuiser l'espace de numéros de séquence à 32 bits de ESP, exigeant de fréquents changements de clé de la SA, car le retour à zéro des numéros de séquence ESP au sein d'une seule SA est prohibé aussi bien pour ESPv2 [RFC2406] que ESPv3 [RFC4303]. Afin de fournir le moyen d'éviter ce changement de clés fréquent potentiellement indésirable, les mises en œuvre qui sont capables de fonctionner à des vitesses de 1 gigabit/s ou plus DOIVENT mettre en œuvre les numéros de séquence étendus (64 bits) pour ESPv2 (et ESPv3, si il est pris en charge) et DEVRAIENT utiliser les numéros de séquence étendus pour tout le trafic de protocole de mémorisation de bloc. La négociation de numéro de séquence étendu au titre de l'établissement de l'association de sécurité est spécifiée dans la [RFC4304] pour IKEv1 et dans la [RFC5996] pour IKEv2.

2.1 Transformations d'authentification d'origine des données et d'intégrité des données

La RFC 3723 exige que :

- HMAC-SHA1 DOIT être mis en œuvre sous la forme de HMAC-SHA-1-96 [RFC2404].
- Le MAC CBC AES avec extensions XCBC DEVRAIT être mis en œuvre [RFC3566].

Le présent document précise les exigences de taille de clés de la RFC 3723 pour les mises en œuvre de MAC CBC AES avec extensions XCBC ; les clés de 128 bits DOIVENT être prises en charge, et d'autres tailles de clés PEUVENT aussi être prises en charge.

Le présent document ajoute aussi une exigence pour IPsec v3 :

- Les mises en œuvre qui prennent en charge IKEv2 [RFC5996] DEVRAIENT aussi mettre en œuvre le GMAC AES [RFC4543]. Les mises en œuvre de AES GMAC DOIVENT prendre en charge les clés de 128 bits et PEUVENT prendre en charge d'autres tailles de clés.

La raison de l'ajout de cette exigence est que GMAC est plus convenable pour les mises en œuvre de matériels qui peuvent être préférables pour les hauts débits de données auxquels les protocoles de mémorisation de bloc sont supposés fonctionner.

2.2 Exigences de transformation de confidentialité

La RFC 3723 exige que :

- 3DES en mode CBC (3DES CBC) [RFC2451] [triple-des-spec] DOIT être pris en charge.
- AES en mode compteur (AES CTR) [RFC3686] DEVRAIT être pris en charge.
- Le chiffrement NUL [RFC2410] DOIT être pris en charge.

Les exigences ci-dessus, tirées de la RFC 3723 concernant 3DES CBC et AES CTR sont remplacées dans le présent document par l'exigence que 3DES CBC et AES CTR PEUVENT tous deux être mis en œuvre. L'exigence du chiffrement NUL n'est pas changée par le présent document. L'exigence de 3DES CBC correspondait à l'exigence d'interopérabilité du chiffrement de base pour IPsec v2. Au moment de la publication de la RFC 3723, AES en mode compteur était la transformation de chiffrement qui convenait le mieux aux mises en œuvre de matériel, car une mise en œuvre de matériel peut être préférable pour les hauts débits de données auxquels un protocole de mémorisation de bloc peut être supposé fonctionner. Le présent document change ces deux exigences, sur la base des développements de la cryptographie depuis la publication de la RFC 3723.

L'exigence de 3DES CBC est devenue problématique due à la taille de bloc de 64 bits de 3DES ; c'est-à-dire que le cœur de chiffrement chiffre ou déchiffre 64 bits à la fois. Les faiblesses de la sécurité du chiffrement commencent à apparaître lorsque la quantité de données chiffrées sous une seule clé approche de la limite d'anniversaire de 32 Gio (gibioctets) pour un chiffrement d'une taille de bloc de 64 bits ; voir l'Appendice A et [triple-des-birthday]. Il est prudent de changer de clé bien avant d'atteindre cette limite, et 32 Gio ou une fraction significative de cette quantité est moins que la quantité de données qu'un protocole de mémorisation de bloc peut transférer dans une seule session. Cela peut exiger de fréquents changements de clés, par exemple, pour obtenir une marge de sécurité d'ordre de grandeur (10x) en changeant de clé après 3 Gio sur une liaison à plusieurs gigabit/s. À l'opposé, AES a une taille de bloc de 128 bits, qui résulte en une limite d'anniversaire bien plus grande (2^68 octets); voir l'Appendice A. AES CBC [RFC3602] est la principale transformation de chiffrement de mise en œuvee obligatoire pour l'interopérabilité et est donc la transformation de mise en œuvre obligatoire appropriée de remplacement pour 3DES CBC.

AES en mode compteur (AES CTR) n'est plus la transformation de chiffrement qui est la plus convenable pour une mise en œuvre de matériel. Cette caractérisation s'applique maintenant à AES GCM [RFC4106], qui fournit à la fois le chiffrement et la protection de l'intégrité dans un seul mécanisme cryptographique (à l'opposé, ni HMAC-SHA1 ni AES CBC MAC avec extensions XCBC ne conviennent bien pour une mise en œuvre de matériel, car les deux transformations ne fonctionnent pas bien en parallèle). AES GCM est aussi capable de fournir la protection de la confidentialité pour le protocole d'échange IKEv2, mais pas le protocole IKEv1 [RFC5282], et donc la nouvelle exigence d'AES GCM "DEVRAIT" se fonde sur la présence de la prise en charge de IKEv2.

Pour les raisons décrites aux paragraphes précédents, les exigences de transformation de confidentialité de la RFC 3723 sont remplacées par ce qui suit :

- 3DES en mode CBC PEUT être mis en œuvre (remplace l'exigence "DOIT mettre en œuvre" de la RFC 3273).
- AES en mode compteur (AES CTR) PEUT être mis en œuvre (remplace l'exigence "DEVRAIT mettre en œuvre" de la RFC 3273).
- AES en mode CBC DOIT être mis en œuvre. Les mises en œuvre AES CBC DOIVENT prendre en charge les clés de 128 bits et PEUVENT prendre en charge d'autres tailles de clés.
- Les mises en œuvre qui prennent en charge IKEv2 DEVRAIENT aussi mettre en œuvre AES GCM. Les mises en œuvre AES GCM DOIVENT prendre en charge les clés de 128 bits et PEUVENT prendre en charge d'autres tailles de clés.
- Le chiffrement NUL [RFC2410] DOIT être pris en charge.

L'exigence de la prise en charge du chiffrement NUL permet l'utilisation des SA qui fournissent l'authentification de l'origine des données et l'intégrité des données, mais pas la confidentialité.

D'autres transformations PEUVENT être mises en œuvre en plus de celles mentionnées ci-dessus.

3. Exigences pour IKEv1 et IKEv2

Note : Pour éviter les ambiguïtés, le protocole IKE d'origine [RFC2409] est appelé "IKEv1" dans le présent document.

Le présent document ajoute des exigences pour l'utilisation de IKEv2 avec les protocoles de mémorisation de bloc et fait les deux changements suivants aux exigences de IKEv1 de la RFC 3723 (l'exigence du nouveau groupe Diffie-Hellman (DH) s'applique aussi à IKEv2) :

- Quand des groupes DH sont utilisés, un groupe DH d'au moins 2048 bits DEVRAIT être offert au titre des propositions de créer des associations de sécurité IPsec. La recommandation de l'utilisation de groupes DH de 1024 bits avec 3DES CBC et HMAC-SHA1 a été supprimée ; l'utilisation de groupes DH de 1024 bits N'EST PAS RECOMMANDÉE, et
- L'exigence d'utiliser l'accès UDP 500 est supprimée afin de permettre la traversée des NAT [RFC3947].

Il n'y a pas d'autre changement aux exigences IKEv1 de la RFC 3723, mais beaucoup d'entre elles sont répétées dans le présent document afin de fournir le contexte des nouvelles exigences IKEv2.

La RFC 3723 exige que IKEv1 [RFC2409] soit pris en charge pour l'authentification de l'homologue, la négociation des associations de sécurité, et la gestion de clés, en utilisant le domaine d'interprétation (DOI) IPsec [RFC2407], et elle exige de plus que le changement de clés manuel ne soit pas utilisé car il ne fournit pas la prise en charge de changement de clés nécessaire pour le fonctionnement à haut débit. Le présent document ajoute l'exigence que IKEv2 [RFC5996] DEVRAIT être pris en charge pour l'authentification de l'homologue, la négociation des associations de sécurité, et la gestion de clés. L'interdiction du changement de clés manuel comme prévu dans la RFC 3723 est étendu à IKEv2 ; le changement de clés manuel NE DOIT PAS être utilisé avec toute version de IPsec pour les protocoles auxquels les exigences du présent document s'appliquent.

Les exigences de la RFC 3723 pour la mise en œuvre et l'usage du mode IKEv1 sont inchangées ; le présent document n'étend pas ces exigences à IKEv2 parce que IKEv2 n'a pas de modes.

Quand IPsec est utilisé, la réception d'un message IKEv1 phase 2 qui supprime le message, ou de l'échange IKEv2 INFORMATION qui supprime la SA, NE DEVRAIT PAS être interprétée comme une raison pour supprimer la connexion du protocole de mémorisation de bloc (par exemple, fondée sur TCP). Si du trafic supplémentaire est envoyé, une nouvelle SA sera créée pour protéger ce trafic.

La méthode utilisée pour déterminer si une connexion de protocole de mémorisation de bloc devrait être établie en utilisant IPsec est considérée comme un problème d'administration de politique IPsec et n'est donc pas définie dans le présent document. La méthode utilisée par une mise en œuvre qui prend en charge les deux versions IPsec v2 et v3 pour déterminer quelles versions de IPsec sont prises en charge par un protocole de mémorisation de bloc d'homologue est aussi considérée comme une question d'administration de politique IPsec et n'est donc pas définie dans le présent document. Si IPsec v2 et v3 sont toutes deux prises en charge par les deux points d'extrémité d'une connexion de protocole de mémorisation de bloc, l'utilisation de IPsec v3 est RECOMMANDÉE.

3.1 Exigences d'authentification

Les exigences d'authentification pour IKEv1 sont inchangées par le présent document mais sont répétées ici pour le contexte, avec les exigences d'authentification pour IKEv2:

a. L'authentification de l'homologue à l'aide d'une clé de chiffrement prépartagée DOIT être prise en charge. L'authentification de l'homologue fondée sur le certificat en utilisant des signatures numériques PEUT être prise en charge. Pour IKEv1 [RFC2409], l'authentification de l'homologue à l'aide des méthodes de chiffrement à clé publique spécifiée aux paragraphes 5.2 et 5.3 de la [RFC2409] NE DEVRAIT PAS être utilisée.

b. Quand des signatures numériques sont utilisées pour l'authentification, tous les négociateurs IKEv1 et IKEv2 DEVRAIENT utiliser la ou les charges utiles de demande de certificat pour spécifier l'autorité de certification et DEVRAIENT vérifier la validité du certificat via la liste pertinente de révocation de certificat (CRL) ou l'utilisation du

protocole d'état de certificat en ligne (OCSP) [RFC6960] avant d'accepter un certificat PKI dans l'authentification. La prise en charge de OSCP au sein du protocole IKEv2 est spécifiée dans la [RFC4806].

c. Les mises en œuvre IKEv1 DOIVENT prendre en charge le mode principal et DEVRAIENT prendre en charge le mode agressif. Le mode principal avec la méthode d'authentification à clés prépartagées NE DEVRAIT PAS être utilisé quand l'initiateur ou la cible utilise des adresses IP allouées de façon dynamique. Bien que dans de nombreux cas les clés prépartagées offrent une bonne sécurité, il y a des situations où des adresses allouées de façon dynamique sont utilisées pour forcer l'utilisation d'un groupe de clés prépartagées, qui créent des vulnérabilités à l'attaque par interposition. Ces exigences ne s'appliquent pas à IKEv2 parce qu'il n'a pas de modes.

d. Dans le mode rapide de IKEv1 phase 2, dans les échanges pour la création de SA de phase 2, la charge utile d'identification DOIT être présente. Cette exigence ne s'applique pas à IKEv2 parce qu'il n'a pas de modes.

e. Les exigences de type d'identification suivantes s'appliquent à IKEv1. Les types d'identification ID_IPV4_ADDR, ID_IPV6_ADDR (si la pile de protocoles prend en charge IPv6), et ID_FQDN DOIVENT être pris en charge ; ID_USER_FQDN DEVRAIT être pris en charge. Les types d'identification Sous réseau IP, Gamme d'adresse IP, ID_DER_ASN1_DN, et ID_DER_ASN1_GN NE DEVRAIENT PAS être utilisés. Le type d'identification ID_KEY_ID NE DOIT PAS être utilisé.

f. Quand IKEv2 est pris en charge, le protocole de mémorisation de bloc suivant s'applique. Les types d'identification ID_IPV4_ADDR, ID_IPV6_ADDR (si la pile de protocoles prend en charge IPv6), et ID_FQDN DOIVENT être pris en charge ; ID_RFC822_ADDR DEVRAIT être pris en charge. Les types d'identification ID_DER_ASN1_DN et ID_DER_ASN1_GN NE DEVRAIENT PAS être utilisés. Le type d'identification ID_KEY_ID NE DOIT PAS être utilisé.

Les raisons des protocoles de mémorisation de bloc aux points e et f sont les suivantes :
- Le sous réseau IP et la gamme d'adresses IP sont trop vagues pour identifier utilement un point d'extrémité iSCSI.
- Les types _DN et _GN sont des identités X.500 ; il vaut généralement mieux utiliser une identité tirée d'un subjectAltName dans un certificat PKI.
- ID_KEY_ID est un identifiant opaque qui n'est pas interopérable sur les différentes mises en œuvre IPsec comme spécifié. L'hétérogénéité dans certaines mises en œuvre de protocole de mémorisation de bloc est prévisible (par exemple, mises en œuvre d'initiateur iSCSI contre mises en œuvre de cible iSCSI) et donc, l'hétérogénéité des mises en œuvre IPsec est importante.

3.2 Exigences pour groupes DH et PRF

Le présent document ne change pas les exigences de prise en charge des groupes Diffie-Hellman (DH) et de fonctions pseudo aléatoires (PRF, *Pseudo-Random Function*). Voir dans la [RFC4109] les exigences pour IKEv1 et dans la [RFC4307] les exigences pour IKEv2. Il est conseillé aux développeurs de vérifier les RFC suivantes qui mettront à jour ces RFC, car de telles mises à jour pourraient changer ces exigences.

Quand des groupes DH sont utilisés, un groupe DH d'au moins 2048 bits DEVRAIT être offert au titre de toutes les propositions de créer des associations de sécurité IPsec pour IKEv1 comme pour IKEv2.

La RFC 3723 exige que la prise en charge du secret parfait vers l'avant dans l'échange de clé en mode rapide IKEv1 DOIT être mis en œuvre. Le présent document étend cette exigence à IKEv2 ; la prise en charge du secret parfait vers l'avant dans l'échange de clé CREATE_CHILD_SA DOIT être mise en œuvre pour l'utilisation de IPsec avec un protocole de mémorisation de bloc.

4. Considérations sur la sécurité

Ce document est tout entier consacré à la sécurité.

Les sections "Considérations sur la sécurité" de toutes les RFC référencées s'appliquent, et une attention particulière devrait être portée aux considérations sur la sécurité des transformations de chiffrement dont les niveaux d'exigence sont changés par la présente RFC :
- AES GMAC [RFC4543] (nouvelle exigence -- DEVRAIT être pris en charge quand IKEv2 est pris en charge),
- 3DES CBC [RFC2451] (changé de "DOIT être pris en charge" à "PEUT être pris en charge"),
- AES CTR [RFC3686] (changé de "DEVRAIT être pris en charge" à "PEUT être pris en charge"),

- AES CBC [RFC3602] (nouvelle exigence -- DOIT être pris en charge), et
- AES GCM [RFC4106] (nouvelle exigence -- DEVRAIT être pris en charge quand IKEv2 est pris en charge).

Les considérations sur la sécurité concernant l'utilisation de AES GCM [RFC4106] et AES GMAC [RFC4543] sont d'un intérêt particulier ; les deux modes sont vulnérables à des attaques de tromperie catastrophiques si un nom occasionnel est répété avec une certaine clé.

Le niveau d'exigence pour 3DES CBC a été réduit, sur la base des considérations sur les mises en œuvre à haut débit ; 3DES CBC reste une transformation de chiffrement facultative qui peut convenir pour les mises en œuvre limitées au fonctionnement à des débits inférieurs où la fréquence de changement de clé requise pour 3DES est acceptable.

Le niveau d'exigence pour AES CTR a été réduit, sur la seule base des considérations de mise en œuvre de matériel qui priviligient AES GCM, par opposition aux changements des propriétés de sécurité de AES CTR. AES CTR reste une transformation de sécurité facultative qui convient pour une utilisation générale, car il ne partage pas l'exigence de 3DES CBC d'un changement fréquent de clés quand il fonctionne à de hauts débits de données.

Des tailles de clés d'une force comparable DEVRAIENT être utilisées pour les algorithmes et transformations de chiffrement pour toute association de sécurité IPsec individuelle. Voir les détails au paragraphe 5.6 de [SP800-57].

5. Références

5.1 Références normatives

[RFC2119] S. Bradner, "Mots clés à utiliser dans les RFC pour indiquer les niveaux d'exigence", BCP 14, mars 1997. *(MàJ par* RFC8174)

[RFC2401] S. Kent et R. Atkinson, "Architecture de sécurité pour le protocole Internet", novembre 1998. (*Obsolète, voir* RFC4301)

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

[RFC2406] S. Kent et R. Atkinson, "Encapsulation de charge utile de sécurité IP (ESP)", novembre 1998. *(Ob., voir* RFC4303)

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

[RFC2409] D. Harkins et D. Carrel, "L'échange de clés Internet (IKE)", novembre 1998. *(Obsolète, voir la* RFC4306)

[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. *(P.S.)*

[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.)*

[RFC3720] J. Satran et autres, "Interface Internet des systèmes de petits ordinateurs (iSCSI)", avril 2004. *(Remplacée par* RFC7143)

[RFC3723] B. Aboba et autres, "Protocoles de sécurisation de mémorisation de blocs sur IP", avril 2004. *(P.S.)*

[RFC3821] M. Rajagopal, E. Rodriguez, R. Weber, "Canal fibre sur TCP/IP (FCIP)", juillet 2004. *(P.S.)*

[RFC3822] D. Peterson, "Découverte de canal fibre sur des entités TCP/IP (FCIP) en utilisant le protocole de localisation de service version 2 (SLPv2)", juillet 2004. *(P.S.)*

[RFC3947] T. Kivinen et autres, "Négociation de traversée de NAT dans IKE", janvier 2005. *(P.S.)*

[RFC4018] M. Bakke et autres, "Découverte de cibles et des serveurs de noms des interfaces Internet de systèmes de petits ordinateurs (iSCSI) en utilisant le protocole de localisation de service version 2 (SLPv2)", avril 2005. *(P.S.) (MàJ par* RFC7146)

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

[RFC4109] P. Hoffman, "Algorithmes pour la version 1 de l'échange de clés Internet (IKEv1)", mai 2005. (*MàJ* RFC2409) *(P.S.)*

[RFC4172] C. Monia et autres, "iFCP – un protocole pour le réseautage des mises en mémoire de canal fibre sur Internet", septembre 2005. *(P.S.)*

[RFC4173] P. Sarkar et autres, "Clients d'amorçage qui utilisent le protocole d'interface Internet de système de petit ordinateur (iSCSI)", septembre 2005. *(P.S.)*

[RFC4174] C. Monia et autres, "Option IPv4 du protocole de configuration dynamique d'hôte (DHCP) pour le service de noms de mémorisation sur Internet", septembre 2005. *(P.S.)*

[RFC4301] S. Kent et K. Seo, "Architecture de sécurité pour le protocole Internet", décembre 2005. *(P.S.) (Remplace la* RFC2401)

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

[RFC4304] S. Kent, "Addendum du numéro de séquence étendu (ESN) au domaine d'interprétation IPsec (DOI) pour le protocole d'associations de sécurité et de gestion de clé Internet (ISAKMP)", décembre 2005. *(P.S.)*

[RFC4307] J. Schiller, "Algorithmes cryptographiques à utiliser avec la version 2 de l'échange de clés sur Internet (IKEv2)", décembre 2005. *(P.S. ; rendue obsolète par* RFC8247)

[RFC4543] D. McGrew, J. Viega, "Utilisation du code d'authentification de message de Galois (GMAC) dans les ESP et AH d'IPsec", mai 2006. *(P.S.)*

[RFC5040] R. Recio et autres, "Spécification d'un protocole d'accès direct à une mémoire distante", octobre 2007. *(P.S.)*

[RFC5041] H. Shah et autres, "Placement direct des données sur transports fiables", octobre 2007. *(P.S.)*

[RFC5042] J. Pinkerton, E. Deleganes, "Sécurité du protocole de placement direct des données (DDP) / protocole d'accès direct à une mémoire distante (RDMAP)", octobre 2007. *(P.S.)*

[RFC5043] C. Bestler et R. Stewart, éd., "Adaptation du placement direct des données (DDP) au protocole de transmission de contrôle de flux (SCTP)", octobre 2007. (*MàJ par la* RFC6581) *(P.S.)*

[RFC5044] P. Culley et autres, "Tramage verrouillé sur la PDU de marqueur pour la spécification de TCP", octobre 2007. (*MàJ par la* RFC6581) *(P.S.)*

[RFC5045] C. Bestler et autres, "Applicabilité du protocole d'accès direct à une mémoire distante (RDMA) et du placement direct des données (DDP)", octobre 2007. *(Information)*

[RFC5046] M. Ko et autres, "Extensions pour l'accès direct à une mémoire distante (RDMA) à l'interface Internet de système de petit ordinateur (iSCSI)", octobre 2007. *(P.S.) (Remplacée par* RFC7145)

[RFC5047] M. Chadalapaka et autres, "DA : Architecture Datamover pour l'interface Internet de système de petit ordinateur (iSCSI)", octobre 2007. *(Information)*

[RFC5048] M. Chadalapaka, éd. "Corrections et précisions à l'interface Internet de système de petit ordinateur (iSCSI)", octobre 2007. (*MàJ* RFC3720) *(P.S.) (Remplacée par* RFC7143)

[RFC5282] D. Black, D. McGrew, "Utilisation des algorithmes de chiffrement authentifiés avec la charge utile du protocole d'échange de clé Internet version 2 (IKEv2)", août 2008. (*MàJ* RFC4306) *(P.S.)*

[RFC5996] C. Kaufman, P. Hoffman, Y. Nir, P. Eronen, "Protocole d'échange de clés sur Internet, version 2 (IKEv2)", septembre 2010 (*Remplace* RFC4306, RFC4718) (*MàJ par* RFC5998) *(P.S.)*

[RFC6960] S. Santesson et autres, "Protocole d'état de certificat en ligne (OCSP) pour l'infrastructure de clé publique Internet X.509", juin 2013. (*Remplace* RFC2560, 6277) (*MàJ* RFC5912) *(P.S.)*

[RFC7143] M. Chadalapaka et autres, "Protocole (consolidé) d'interface Internet de petit système d'ordinateur (iSCSI)", avril 2014. (*Remplace* RFC3720, 3980, 4850, 5048) (*MàJ* RFC3721) *(P.S.)*

[RFC7145] M. Ko, A. Nezhinsky, "Extensions d'interface Internet de petit système d'ordinateur (iSCSI) pour la spécification d'accès direct à une mémore distante (RDMA)", avril 2014. (*Remplace* RFC5046) *(P.S.)*

[SP800-57] Barker, E., Barker, W., Burr, W., Polk, W., and M. Smid, "NIST Special Publication 800-57: Recommendation for Key Management - Part 1: General (Revision 3)", juillet 2012, <http://csrc.nist.gov/publications/nistpubs/800-57/sp800-57_part1_rev3_general.pdf >.

[triple-des-birthday] McGrew, D., "Impossible plaintext cryptanalysis and probable-plaintext collision attacks of 64-bit block cipher modes (Cryptology ePrint Archive: Report 2012/623)", novembre 2012, <http://eprint.iacr.org/2012/623>.

[triple-des-spec] American Bankers Association (ABA), "American National Standard for Financial Services X9.52-1998 - Triple Data Encryption Algorithm Modes of Operation", juillet 1998.

5.2 Références pour information

[RFC3721] M. Bakke et autres, "Interface Internet des systèmes de petits ordinateurs (iSCSI) : dénomination et découverte", avril 2004. *(Information) (MàJ par* RFC7143)

[RFC4806] M. Myers, H. Tschofenig, "Extensions du protocole d'état de certificat en ligne (OCSP) à IKEv2", février 2007. *(P.S.)*

[RFC5045] C. Bestler et autres, "Applicabilité du protocole d'accès direct à une mémoire distante (RDMA) et du placement direct des données (DDP)", octobre 2007. *(Information)*

[RFC5047] M. Chadalapaka et autres, "DA : Architecture Datamover pour l'interface Internet de système de petit ordinateur (iSCSI)", octobre 2007. *(Information)*

[RFC5387] J. Touch et autres, "Problème et déclaration d'applicabilité pour la sécurité mieux que rien (BTNS)", novembre 2008. *(Info.)*

Appendice A. Limites d'anniversaire de chiffrement de bloc

Le présent appendice donne les limites d'anniversaire pour les chiffrements 3DES et AES sur la base de [triple-des-birthday], qui déclare : "La théorie se prononce contre l'utilisation d'un chiffrement de bloc de w bits pour chiffrer plus de 2^(w/2) blocs avec une seule clé ; ceci est connu sous le nom de limite d'anniversaire".

Pour un chiffrement avec une taille de bloc de 64 bits (par exemple, 3DES), w = 64, de sorte que la limite d'anniversaire est 2^32 blocs. Comme chaque bloc contient 8 (2^3) octets, la limite d'anniversaire est 2^35 octets = 2^5 gibioctets, c'est-à-dire, 32 GiB, où un gibioctet (Gio) = 2^30 octets. Noter qu'un gigaoctet (quantité décimale) n'est pas la même chose qu'un gibioctet (quantité binaire) ; 1 gigaoctet (GB) = 10^6 octets.

Pour un chiffrement avec une taille de bloc de 128 bits (par exemple, AES), w = 128, de sorte que la limite d'anniversaire est 2^64 blocs. Comme chaque bloc contient 16 (2^4) octets, la limite d'anniversaire est 2^68 octets = 2^8 exbioctets, cest-à-dire, 256 Eio, où un exbioctet (Eio) = 2^60 octets. Noter qu'un exaoctet (quantité décimale) n'est pas la même chose qu'un exbioctet (quantité binaire) ; 1 exaoctet (EB) = 10^9 octets.

Appendice B. Contributeurs

Les observations de David McGrew sur les implications pour les limites d'anniversaire de la taille du bloc de 64 bits de 3DES, faites sur la liste de diffusion ipsec@ietf.org nous ont conduit à changer du CBC 3DES au CBC AES comme algorithme de chiffrement de mise en œuvre obligatoire, sur la base de la discussion des limites d'anniversaire de l'Appendice A.

Les auteurs de la RFC 3723 d'origine étaient Bernard Aboba, Joshua Tseng, Jesse Walker, Venkat Rangan, et Franco Travostino. Des commentaires de Francis Dupont, Yaron Sheffer, Tom Talpey, Sean Turner, et Tom Yu ont amélioré ce document et nous les en remercions chaleureusement.

Adresse des auteurs

David L. Black
EMC Corporation
176 South St.
Hopkinton, MA 01748
USA
téléphone : +1 508 293-7953
mél : david.black@emc.com

Paul Koning
Dell
300 Innovative Way
Nashua, NH 03062
USA
téléphone : +1 603 249-7703
mél : paul_koning@Dell.com