Groupe de travail Réseau
Request for Comments : 4309
Catégorie : Sur la voie de la normalisation
Traduction Claude Brière de L'Isle

R. Housley, Vigil Security

décembre 2005

Utilisation du mode CCM de la norme de chiffrement évoluée (AES) avec l'encapsulation de charge utile de sécurité (ESP) d'IPsec

Résumé
Le présent document décrit l'utilisation de la norme de chiffrement évolué (AES, *Advanced Encryption Standard*) en mode compteur avec CBC-MAC (CCM, *Counter with CBC-MAC*) avec une valeur d'initialisation explicite comme mécanisme d'encapsulation de charge de sécurité (ESP, *Encapsulating Security Payload*) IPsec pour assurer la confidentialité, l'authentification de l'origine des données, et l'intégrité sans connexion.

Table des matières

1. Introduction

La norme de chiffrement évolué (AES, *Advanced Encryption Standard*) [AES] est un chiffrement de bloc, et elle peut être utilisée dans de nombreux modes différents. Le présent document décrit l'utilisation de AES en mode compteur avec CBC-MAC (CCM, *Counter with CBC-MAC*) (AES CCM) avec une valeur d'initialisation (IV, *initialization vector*) explicite, comme mécanisme d'encapsulation de charge utile de sécurité (ESP, *Encapsulating Security Payload*) [RFC4303] IPsec pour assurer la confidentialité, l'authentification de l'origine des données, et l'intégrité sans connexion.

Le présent document ne fait pas de présentation d'IPsec. Cependant, des informations sur la façon dont les divers composants d'IPsec fournissent collectivement les services de sécurité se trouvent dans les [RFC4301] et [RFC2411].

1.1 Conventions utilisées dans le document

Les mots clés "DOIT", "NE DOIT PAS", "EXIGE", "DEVRA", "NE DEVRA PAS", "DEVRAIT", "NE DEVRAIT PAS", "RECOMMANDE", "PEUT", et "FACULTATIF" en majuscules dans ce document sont à interpréter comme décrit dans le BCP 14, [RFC2119].

2. Mode AES CCM

CCM est un mode de chiffrement de bloc générique d'authentification et de chiffrement [RFC3610]. Dans la présente spécification, CCM est utilisé avec le mode de chiffrement de bloc AES [AES].

CCM AES a deux paramètres :

M : M indique la taille de la valeur de contrôle d'intégrité (ICV, *integrity check value*). CCM définit des valeurs de 4, 6, 8, 10, 12, 14, et 16 octets ; Cependant, pour conserver l'alignement et fournir une sécurité adéquate, seules les valeurs qui sont un multiple de quatre et supérieures à huit sont permises. Les mises en œuvre DOIVENT prendre en charge les valeurs de M de 8 et 16 octets, et les mises en œuvre PEUVENT prendre en charge une valeur de M de 12 octets.

L : L indique la taille du champ Longueur en octets. CCM définit les valeurs de L entre 2 octets et 8 octets. La présente spécification ne prend en charge que L = 4. Les mises en œuvre DOIVENT prendre en charge une valeur de L de 4 octets, qui s'accommode d'un jumbogramme complet [RFC2675] ; cependant, la longueur inclut toutes les données chiffrées, ce qui inclut aussi les champs Bourrage ESP, Longueur de bourrage, et Prochain en-tête.

Il y a quatre entrées au traitement du générateur de CCM :

clé : une seule clé est utilisée pour calculer l'ICV en utilisant CBC-MAC et pour effectuer le chiffrement de la charge utile en utilisant le mode compteur. AES prend en charge des tailles de clé de 128 bits, 192 bits, et 256 bits. La taille de clé par défaut est 128 bits, et les mises en œuvre DOIVENT prendre en charge cette taille de clé. Les mises en œuvre PEUVENT aussi prendre en charge des tailles de clé de 192 bits et 256 bits.

nom occasionnel *(nonce)* : la taille du nom occasionnel dépend de la valeur choisie pour le paramètre L. Il est de 15 L octets. Les mises en œuvre DOIVENT prendre en charge un nom occasionnel de 11 octets. La construction du nom occasionnel est décrite à la Section 4.

charge utile : la charge utile du paquet ESP. Elle NE DOIT PAS faire plus de 4 294 967 295 octets, qui est la taille maximum d'un jumbogramme [RFC2675] ; cependant, les champs Bourrage ESP, Longueur de bourrage, et Prochain en-tête font aussi partie de la charge utile.

AAD : CCM assure l'intégrité des données et l'authentification de l'origine des données pour certaines données en dehors de la charge utile. CCM ne permet pas que des données authentifiées supplémentaires (AAD, *additional authenticated data*) fassent plus de 18 446 744 073 709 551 615 octets. La ICV est calculée à partir des champs d'en-tête ESP, de charge utile ESP, et d'en-queue ESP, ce qui est significativement plus court que la limite imposée par CCM. La construction des AAD est décrite à la Section 5.

AES CCM exige que le chiffreur génère une valeur unique par paquet et communique cette valeur au déchiffreur.Cette valeur par paquet est une des parties composantes du nom occasionnel, et on l'appelle la valeur d'initialisation (IV, *initialization vector*). La même combinaison d'IV et de clé NE DOIT PAS être utilisée plus d'une fois. Le chiffreur peut générer la IV de toute façon qui assure l'unicité. Les approches courantes de génération d'IV incluent d'incrémenter un compteur pour chaque paquet et registres à décalage avec réinjection linéaire (LFSR, *linear feedback shift register*).

AES CCM emploie le mode compteur pour le chiffrement. Comme avec tout chiffrement de flux, la réutilisation de la même valeur d'IV avec la même clé est catastrophique. Une collision d'IV fait immédiatement une fuite d'informations sur les textes en clair des deux paquets. Pour cette raison, il est inapproprié d'utiliser ce CCM avec des clés à configuration statique. Des mesures extraordinaires seraient nécessaires pour empêcher la réutilisation d'une valeur d'IV avec la clé statique à travers les cycles d'alimentation. Pour être sûres, les mises en œuvre DOIVENT utiliser des clés fraîches avec

AES CCM. Le protocole d'échange de clés Internet (IKE, *Internet Key Exchange*) [IKE] ou IKEv2 [RFC4306] peut être utilisé pour établir des clés fraîches.

3. Charge utile ESP

La charge utile ESP est composée de l'IV suivi par le texte chiffré. Le champ Charge utile, comme défini dans la [RFC4303], est structuré comme le montre la Figure 1.

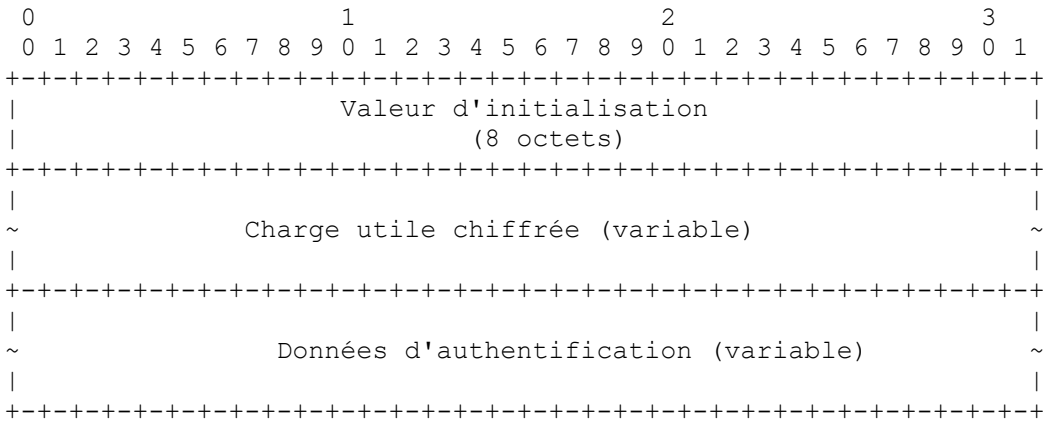

Figure 1 : Charge utile ESP chiffrée avec AES CCM

3.1 Valeur d'initialisation (IV)

Le champ IV AES CCM DOIT faire huit octets. L'IV DOIT être choisie par le chiffreur d'une manière qui assure que la même valeur d'IV est utilisée une seule fois pour une certaine clé. Le chiffreur peut générer l'IV de toute manière qui assure l'unicité. Les approches courantes de la génération d'IV incluent d'incrémenter un compteur pour chaque paquet et des registres à décalage avec réinjection linéaire (LFSR, *linear feedback shift register*).

Inclure l'IV dans chaque paquet assure que le déchiffreur peut générer le flux de clés nécessaire pour le déchiffrement, même quand certains datagrammes sont perdus ou réordonnés.

3.2 Charge utile chiffrée

La charge utile chiffrée contient le texte chiffré.

Le mode AES CCM n'exige pas le bourrage du texte source. Cependant, ESP exige un bourrage pour aligner les données d'authentification sur le mot de 32 bits. Les champs Bourrage, Longueur de bourrage, et Prochain en-tête DOIVENT être enchaînés avec le texte source avant d'effectuer le chiffrement, comme décrit dans la [RFC4303]. Lorsque un bourrage est exigé, il DOIT être généré et vérifié conformément aux conventions spécifiées dans la [RFC4303].

3.3 Données d'authentification

AES CCM fournit une ICV chiffrée. L'ICV fournie par CCM est porté edans les champs Données d'authentification sans autre chiffrement. Les mises en œuvre DOIVENT prendre en charge des tailles d'ICV de 8 octets et 16 octets. Les mises en œuvre PEUVENT aussi prendre en charge des ICV de 12 octets.

4. Format de nom occasionnel

Chaque paquet porte la IV qui est nécessaire pour construire la séquence de blocs de compteur utilisés par le mode compteur pour générer le flux de clés. Le bloc de compteur AES est de 16 octets. Un octet est utilisé pour les fanions CCM, et 4 octets sont utilisés pour le compteur de blocs, comme spécifié par le paramètre CCM L. Les octets restants sont le nom occasionnel. Ces octets occupent du second au douzième octet dans le bloc de compteur. La Figure 2 montre le format du nom occasionnel.

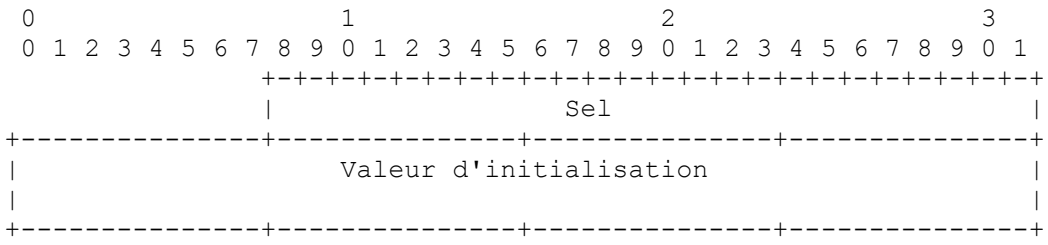

Figure 2. Format de nom occasionnel

Les composants du nom occasionnel sont :

Sel : le champ Sel fait 24 bits. Comme son nom l'indique, il contient une valeur imprévisible. Il DOIT être alloué au début de l'association de sécurité. La valeur de sel n'a pas besoin d'être secrète, mais elle NE DOIT PAS être prévisible avant le début de l'association de sécurité.

Valeur d'initialisation : le champ IV fait 64 bits. Comme décrit au paragraphe 3.1, l'IV DOIT être choisie par le chiffreur d'une manière qui assure que la même valeur d'IV n'est pas utilisée deux fois pour une certaine clé.

Cette construction permet que chaque paquet comporte jusqu'à 2^32 blocs = 4 294 967 296 blocs, = 68 719 476 736 octets.

Cette construction donne plus de flux de clés pour chaque paquet qu'il n'est nécessaire pour traiter un jumbogramme IPv6 [RFC2675].

5. Construction AAD

La protection de l'intégrité des données et l'authentification de l'origine des données pour les champs Indice de paramètres de sécurité (SPI, *Security Parameters Index*) et Numéro de séquence (étendu) sont fournies sans qu'ils soient chiffrés. Deux formats sont définis : un pour les numéros de séquence à 32 bits et un pour les numéros de séquence étendus à 64 bits. Le format avec les numéros de séquence à 32 bits est montré à la Figure 3, et le format avec les numéros de séquence étendus à 64 bits est montré Figure 4.

Les numéros de séquence sont portés dans l'ordre canonique des octets du réseau. Les numéros de séquence étendus sont portés dans l'ordre canonique des octets du réseau, en plaçant d'abord les 32 bits de poids fort et en second les 32 bits de moindre poids. L'ordre canonique des octets du réseau est décrit dans l'appendice B de la RFC0791 (Protocole Internet).

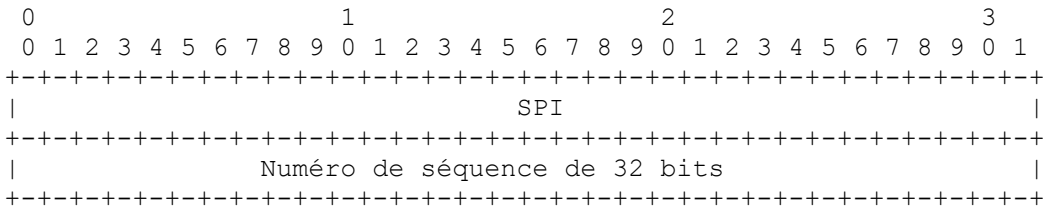

Figure 3. Format AAD avec numéro de séquence de 32 bits

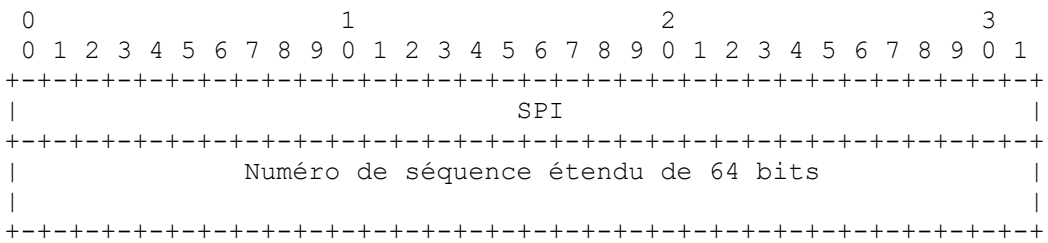

Figure 4. Format AAD avec numéro de séquence étendu de 64 bits

6. Expansion de paquet

La valeur d'initialisation (IV, *Initialization Vector*) et la valeur de contrôle d'intégrité (ICV, *Integrity Check Value*) sont les seules sources d'expansion de paquet. La IV ajoute toujours 8 octets au début de la charge utile. La ICV est ajoutée à la fin de la charge utile, et le paramètre CCM M détermine la taille de l'ICV. Les mises en œuvre DOIVENT prendre en charge les valeur de M de 8 et 16 octets, et les mises en œuvre PEUVENT aussi prendre en charge une valeur de M de 12 octets.

7. Conventions d'IKE

Cette section décrit les conventions utilisées pour générer le matériel de chiffrement et les valeurs de sel à utiliser avec AES CCM en se servant du protocole d'échange de clés Internet [IKE]. Les identifiants et attributs nécessaires pour négocier une association de sécurité qui utilise AES CCM sont aussi définis.

7.1 Matériel de chiffrement et valeurs de sel

Comme décrit plus haut, les mises en œuvre DOIVENT utiliser des clés fraîches avec AES CCM. IKE peut être utilisé pour établir des clés fraîches. Ce paragraphe décrit les conventions pour obtenir la valeur de sel imprévisible à utiliser dans le nom occasionnel à partir de IKE. Noter que cette convention fournit une valeur de sel qui est secrète et imprévisible.

IKE utilise une fonction pseudo aléatoire (PRF, *Pseudo-Random Function*) pour déduire le matériel de chiffrement. La PRF est utilisée de façon itérative pour déduire du matériel de chiffrement de taille arbitraire, appelé "KEYMAT". Le matériel de chiffrement est extrait de la chaîne de résultat sans considération des limites.

La taille de KEYMAT DOIT être de trois octets de plus que ce qui est nécessaire pour la clé AES associée. Le matériel de chiffrement est utilisé comme suit :

AES CCM avec une clé de 128 bits : le KEYMAT demandé pour chaque clé AES CCM est de 19 octets. Les 16 premiers octets sont la clé AES de 128 bits, et les trois octets restants sont utilisés comme valeur de sel dans le bloc compteur.

AES CCM avec une clé de 192 bits : le KEYMAT demandé pour chaque clé AES CCM est de 27 octets. Les 24 premiers octets sont la clé AES de 192 bits, et les trois octets restants sont utilisés comme valeur de sel dans le bloc compteur.

AES CCM avec une clé de 256 bits : le KEYMAT demandé pour chaque clé AES CCM est de 35 octets. Les 32 premiers octets sont la clé AES de 256 bits, et les trois octets restants sont utilisés comme valeur de sel dans le bloc compteur.

7.2 Identifiant de phase 1

Le présent document ne spécifie pas les conventions pour l'utilisation de AES CCM pour les négociations de IKE phase 1. Pour que AES CCM soit utilisé de cette manière, une spécification séparée est nécessaire, et l'identifiant d'algorithme de chiffrement doit être alloué.

7.3 Identifiant de phase 2

Pour les négociations de IKE phase 2, l'IANA a alloué trois identifiants de transformation ESP pour AES CCM avec une IV explicite :

14 pour AES CCM avec une ICV de 8 octets ;
15 pour AES CCM avec une ICV de 12 octets ;
16 pour AES CCM avec une ICV de 16 octets.

7.4 Attribut Longueur de clé

Parce que AES accepte trois longueurs de clé, l'attribut Longueur de clé DOIT être spécifié dans l'échange IKE phase 2 [RFC2407]. L'attribut Longueur de clé DOIT avoir une valeur de 128, 192, ou 256.

8. Vecteurs d'essai

La Section 8 de la [RFC3610] donne des vecteurs d'essais qui vont aider les mises en œuvre du mode AES CCM.

9. Considérations sur la sécurité

AES CCM emploie le mode compteur (CTR) pour la confidentialité. Si une valeur de compteur est utilisée pour plus d'un paquet avec la même clé, alors le même flux de clé sera utilisé pour chiffrer les deux paquets, et il n'y aura plus aucune garantie de confidentialité.

Que se passe t-il si le chiffreur applique l'opérateur OUX au même flux de clés avec deux paquets de texte source différents ? Supposons deux paquets définis par deux séquences d'octets de texte source P1, P2, P3 et Q1, Q2, Q3, et tous deux soient chiffrés avec les flux de clés K1, K2, K3. Les deux textes chiffrés correspondants sont :

(P1 OUX K1), (P2 OUX K2), (P3 OUX K3)

(Q1 OUX K1), (Q2 OUX K2), (Q3 OUX K3)

Si ces deux flux de texte chiffré sont exposés à un attaquant, il en résulte une défaillance catastrophique de la confidentialité parce que :

(P1 OUX K1) OUX (Q1 OUX K1) = P1 OUX Q1
(P2 OUX K2) OUX (Q2 OUX K2) = P2 OUX Q2
(P3 OUX K3) OUX (Q3 OUX K3) = P3 OUX Q3

Une fois que l'attaquant a obtenu les deux textes source OUixés ensemble, il est relativement facile de les séparer. Donc, l'utilisation de tout chiffrement de flux, incluant AES CTR, pour chiffrer deux textes sources sous le même flux de clés crée une fuite du texte source.

Donc, AES CCM ne devrait pas être utilisé avec des clés à configuration statique. Des mesures extraordinaires seraient nécessaires pour empêcher la réutilisation d'une valeur de bloc compteur avec la clé statique à travers les cycles d'alimentation. Pour être sûres, les mises en œuvre DOIVENT utiliser des clés fraîches avec AES CCM. Le protocole IKE [IKE] peut être utilisé pour établir des clés fraîches.

Quand IKE est utilisé pour établir des clés fraîches entre deux entités homologues, des clés séparées sont établies pour les deux flux de trafic. Si un mécanisme différent est utilisé pour établir des clés fraîches, établissant seulement une clé pour chiffrer les paquets, il y a alors une forte probabilité que les homologues choisissent les mêmes valeurs d'IV pour certains paquets. Donc, pour éviter les collisions de bloc compteur, les mises en œuvre d'ESP qui permettent l'utilisation de la même clé pour chiffrer et déchiffrer les paquets avec le même homologue DOIVENT s'assurer que les deux homologues allouent des valeurs de sel différentes à l'association de sécurité (SA).

Sans considération du mode utilisé, AES avec une clé de 128 bits est vulnérable à l'attaque de l'anniversaire après le chiffrement de 2^64 blocs avec une seule clé. Comme ESP avec des numéros de séquence étendus permet jusqu'à 2^64 paquets dans une seule SA, il y a un potentiel réel que plus de 2^64 blocs soient chiffrés avec une seule clé. Les mises en œuvre DEVRAIENT générer une clé fraîche avant que 2^64 blocs soient chiffrés avec la même clé, ou les mises en œuvre DEVRAIENT utiliser des tailles de clé AES plus longues. Noter que ESP avec des numéros de séquence de 32 bits ne va pas excéder 2^64 blocs même si tous les paquets sont des jumbogrammes de longueur maximum.

10. Raisons du concept

Dans le développement de cette spécification, l'utilisation du champ Numéro de séquence ESP au lieu d'un champ d'IV explicite a été examinée. Cette section documente les raisons du choix d'une IV explicite. Ce choix n'est pas un problème de sécurité cryptographique, car l'une ou l'autre approche empêche les collisions de bloc compteur.

L'utilisation d'une IV explicite n'impose pas la manière dont le chiffreur l'utilise pour allouer la valeur par paquet dans le bloc compteur. Ceci est souhaitable pour plusieurs raisons.

1. Seul le chiffreur peut s'assurer que la valeur n'est pas utilisée pour plus d'un paquet, de sorte qu'il n'y a aucun avantage à choisir un mécanisme qui permette au déchiffreur de déterminer si les valeurs de bloc de compteur entrent en collision. Le dommage de la collision est fait, que le déchiffreur le détecte ou non.

2. L'utilisation des IV explicites permet des ajouts, des LFSR, et toute autre technique qui satisfasse le budget temps du chiffreur, pour autant que cette technique résulte en une valeur unique pour chaque paquet. Les ajouts sont simples et de mise en œuvre directe, mais du fait des reports, ils ne s'exécutent pas de façon constante. Les LFSR offrent une solution de remplacement dont la durée d'exécution est constante.

3. La complexité est sous le contrôle de la mise en œuvre. De plus, le choix d'un déchiffreur par la mise en œuvre ne rend pas le déchiffreur plus ou moins complexe.

4. L'allocation de la valeur de de bloc compteur par paquet doit être dans les limites d'assurance. Certaines mises en œuvre allouent le numéro de séquence à l'intérieur des limites d'assurance, mais d'autres ne le font pas. Une collision de numéros de séquence n'a pas de conséquences sévères, mais, comme décrit à la Section 6, une collision des valeurs de bloc compteur a des conséquences désastreuses.

5. Utiliser le numéro de séquence comme IV est possible dans les architectures où l'allocation de numéro de séquence est effectuée au sein des limites d'assurance. Dans cette situation, le numéro de séquence et le champ IV vont contenir la même valeur.

6. En découplant la IV et le numéro de séquence, les architectures où l'allocation du numéro de séquence est effectuée en dehors des limites d'assurance trouvent leur place.

L'utilisation d'un champ IV explicite découle directement du découplage du numéro de séquence et de la valeur de bloc compteur par paquet. La redondance supplémentaire (64 bits pour le champ IV) est acceptable. Cette redondance est significativement inférieure à celle associée au mode de chaînage du bloc de chiffrement (CBC, *Cipher Block Chaining*). Lorsque il est employé normalement, CBC exige un bloc complet pour l'IV et, en moyenne, la moitié d'un bloc pour le bourrage. Le traitement de la confidentialité de AES CCM avec une IV explicite a une redondance du tiers de celle de AES CBC, et elle est constante pour chaque paquet.

11. Considérations relatives à l'IANA

L'IANA a alloué trois numéros de transformation ESP à utiliser avec AES CCM avec une IV explicite :
14 pour AES CCM avec ICV de 8 octets,
15 pour AES CCM avec ICV de 12 octets,
16 pour AES CCM avec ICV de 16 octets.

12. Remerciements

Doug Whiting et Niels Ferguson ont travaillé avec moi pour développer le mode CCM. Le mode CCM a été développé au titre de l'effort de sécurité de l'IEEE 802.11i. Un des aspects les plus intéressants du mode CCM est qu'il ne s'encombre pas de licences. Je remercie les entreprises qui ont soutenu le développement d'un mode de chiffrement d'authentification libre (par ordre alphabétique) : Hifn, Intersil, MacFergus, RSA Security.

Je remercie aussi Tero Kivinen de sa relecture très complète de ce document.

13. Références

13.1 Références normatives

[AES] NIST, FIPS PUB 197, "Advanced Encryption Standard (AES)," novembre 2001.

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

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

voir 4306)

[RFC3610] D. Whiting, R. Housley, N. Ferguson, "Compteur avec CBC-MAC (CCM)", septembre 2003. *(Information)*

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

13.2 Références pour information

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

[RFC2411] R. Thayer, N. Doraswamy, R. Glenn, "Feuille de route pour la sécurité sur IP", novembre 1998. *(Obs., voir* RFC6071)

[RFC2675] D. Borman, S. Deering, R. Hinden, "Jumbogrammes IPv6", août 1999. *(P.S.)*

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

[RFC4306] C. Kaufman, "Protocole d'échange de clés sur Internet (IKEv2)", décembre 2005. *(Obsolète, voir la* RFC5996)

Adresse de l'auteur

Russell Housley
Vigil Security, LLC
918 Spring Knoll Drive
Herndon, VA 20170
USA

mél : housley@vigilsec.com

Déclaration complète de droits de reproduction

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