Groupe de travail Réseau
Request for Comments : 4106
Catégorie : En cours de normalisation
Traduction Claude Brière de L'Isle

J. Viega, Secure Software, Inc.
D. McGrew, Cisco Systems, Inc.

juin 2005

Utilisation du mode Galois/compteur (GCM) dans l'encapsulation IPsec de charge utile de sécurité (ESP)

Résumé
Le présent mémoire décrit l'utilisation de la norme de chiffrement évolué (AES, *Advanced Encryption Standard*) dans le mode Galois/compteur (CGM, *Galois/Counter Mode*) comme un mécanisme d'encapsulation IPsec de charge utile de sécurité (ESP, *Encapsulating Security Payload*) pour assurer la confidentialité et l'authentification de l'origine des données. Cette méthode peut être mise en œuvre efficacement dans le matériel pour des vitesses de 10 gigabits par seconde et au dessus, et convient bien aussi pour les mises en œuvre de logiciels.

Table des Matières

1. Introduction

Le présent document décrit l'utilisation de AES en mode GCM (AES-GCM) comme un mécanisme IPsec ESP pour la confidentialité et l'authentification de l'origine des données. On se réfère à cette méthode comme AES-GCM-ESP. Ce mécanisme n'est pas seulement efficace et sûr, mais il permet aussi des mises en œuvre à grande vitesse dans le matériel. Donc, AES-GCM-ESP permet des connexions IPsec qui peuvent faire un usage efficace des appareils réseau émergeants à 10 gigabits et 40 gigabits.

Le mode compteur (CTR) est apparu comme la méthode préférée de chiffrement pour les mises en œuvre à grande vitesse. À la différence des modes de chiffrement conventionnels comme le chiffrement par chaînage de bloc (CBC, *Cipher Block Chaining*) et le code d'authentification de message par chaînage de bloc de chiffrement (CBC-MAC, *Cipher Block Chaining Message Authentication Code*) CTR peut être efficacement mis en œuvre à des débits de données élevés parce qu'il peut être traité en parallèle. Le protocole ESP CTR décrit comment ce mode peut être utilisé avec IPsec ESP [RFC3686].

Malheureusement CTR ne fournit pas l'authentification de l'origine des données, et donc, la norme ESP CTR exige l'utilisation d'un algorithme d'authentification de l'origine des données en conjonction avec CTR. Cette exigence est problématique, parce que aucun des algorithmes standard d'authentification de l'origine des données ne peut être efficacement mis en œuvre pour les débits de données élevés. GCM résout ce problème, parce que par dessus le marché, il combine le mode CTR avec un mécanisme sûr, parallélisable, et efficace d'authentification.

Le présent document ne couvre pas les détails de la mise en œuvre de GCM. Ces détails se trouvent dans [GCM], avec les valeurs d'essai.

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. AES-GCM

GCM est un mode de fonctionnement par chiffrement de blocs qui assure à la fois la confidentialité et l'authentification de l'origine des données. Le fonctionnement du chiffrement GCM authentifié a quatre entrées : une clé secrète, une valeur d'initialisation (IV), un texte source, et une entrée pour des données authentifiées supplémentaires (AAD, *additional authenticated data*). Il a deux résultats, un texte chiffré dont la longueur est identique à celle du texte source, et une étiquette d'authentification. Dans ce qui suit, on décrit comment la IV, le texte source, et les AAD sont formés à partir des champs d'ESP, et comment le paquet ESP est formé à partir du texte chiffré et de l'étiquette d'authentification.

ESP définit aussi une IV. Pour être clair, on se réfère à l'IV AES-GCM comme à un nom occasionnel dans le contexte de AES-GCM-ESP. La même combinaison de nom occasionnel et de clé NE DOIT PAS être utilisée plus d'une fois.

Parce que la réutilisation d'une combinaison nom occasionnel/clé détruit les garanties de sécurité du mode AES-GCM, il peut être difficile d'utiliser ce mode en toute sécurité lorsque on utilise des clés configurées de façon statique. Pour le bien de la sécurité, les mises en œuvre DOIVENT utiliser un système automatique de gestion de clés, comme l'échange de clé Internet (IKE, *Internet Key Exchange*) [RFC2409], pour s'assurer que cette exigence est satisfaite.

3. Données de charge utile ESP

Les données de charge utile ESP se composent d'une valeur d'initialisation (IV) de huit octets, suivies par le texte chiffré. Le champ Charge utile, comme défini dans la [RFC2406], est structuré comme indiqué à la Figure 1, avec la valeur de contrôle d'intégrité (ICV, *Integrity Check Value*) associée à la charge utile.

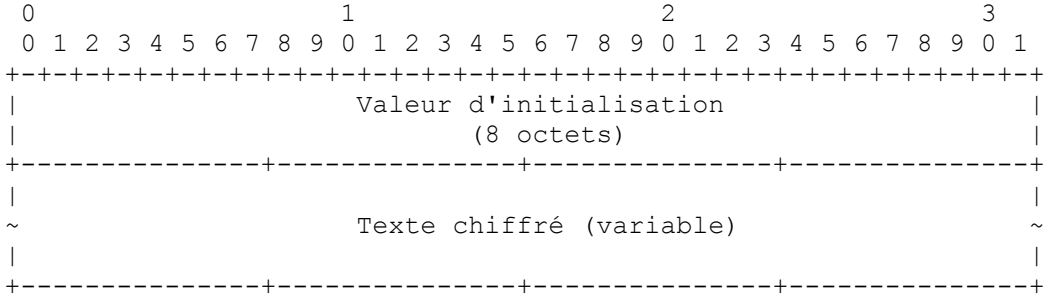

Figure 1 :Charge utile ESP chiffrée avec AES-GCM.

3.1 Valeur d'initialisation (IV)

Le champ IV AES-GCM-ESP DOIT faire huit octets. Pour une clé donnée, la IV NE DOIT PAS se répéter. La façon la plus naturelle de mettre cela en œuvre est avec un compteur, mais tout ce qui peut garantir l'unicité peut être utilisé, comme un registre à décalage avec réinjection linéaire (LFSR, *linear feedback shift register*). Noter que le chiffreur peut utiliser toute méthode de génération d'IV qui satisfait l'exigence d'unicité, sans coordination avec le déchiffreur.

3.2 Texte chiffré

L'entrée de texte source à AES-GCM est formée par l'enchaînement des données du texte source décrites par le champ Prochain en-tête avec les champs Bourrage, Longueur de bourrage, et Prochain en-tête. Le champ Ciphertext consiste en le résultat du texte chiffré à partir de l'algorithme AES-GCM. La longueur du texte chiffré est identique à celle du texte source.

Les mises en œuvre qui ne cherchent pas à cacher la longueur du texte source DEVRAIENT utiliser la quantité minimum de bourrage requise, qui sera de moins de quatre octets.

4. Format de nom occasionnel

Le nom occasionnel passé à l'algorithme de chiffrement GCM-AES a la disposition suivante :

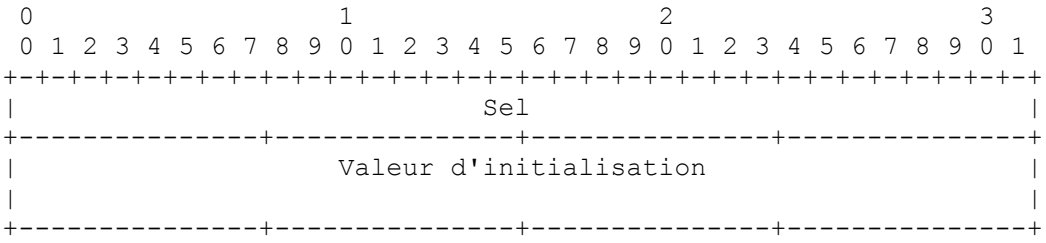

Figure 2 : Format de nom occasionnel

Les composants du nom occasionnel sont les suivants :

Sel : Le champ Sel est une valeur de quatre octets qui est allouée au début de l'association de sécurité, et reste ensuite constante pour toute la vie de l'association de sécurité. Le sel DEVRAIT être imprévisible (c'est-à-dire, choisi au hasard) avant qu'il soit choisi, mais n'a pas besoin d'être secret. On décrit comment régler le sel pour une association de sécurité établie via l'échange de clé Internet au paragraphe 8.1.

Valeur d'initialisation : Le champ IV est décrit au paragraphe 3.1.

5. Construction des AAD

L'authentification de l'intégrité et de l'origine des données pour les champs SPI et Numéro de séquence (étendu) est fournie sans chiffrement. Cela est fait en incluant ces champs dans le champ Données authentifiées supplémentaires (AAD, *Additional Authenticated Data*) AES-GCM. Deux formats d'AAD sont définis : un pour les numéros de séquence de 32 bits, et un pour les numéros de séquence étendus de 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 de 64 bits est montré à la Figure 4.

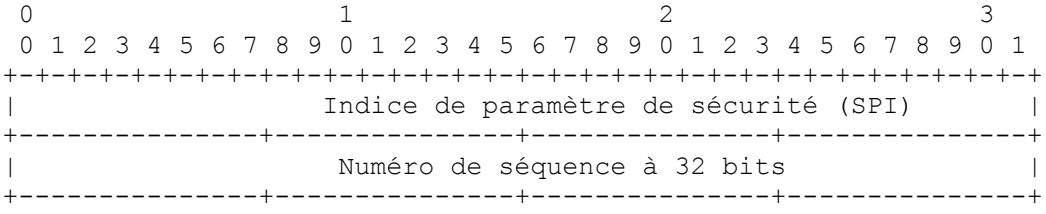

Figure 3 : Format d'AAD avec numéro de séquence de 32 bits

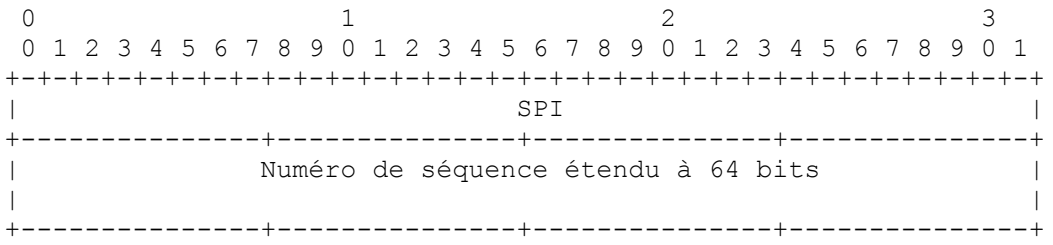

Figure 4 : Format AAD avec numéro de séquence étendu de 64 bits

6. Valeur de contrôle d'intégrité (ICV)

La valeur de contrôle d'intégrité ICV, consiste seulement en l'étiquette d'authentification AES-GCM. Les mises en œuvre DOIVENT prendre en charge une ICV de pleine longueur de 16 octets, et PEUVENT accepter des ICV de 8 ou 12 octets, et NE DOIVENT PAS accepter d'autres longueurs d'ICV. Bien que ESP n'exige pas qu'une ICV soit présente, AES-GCM-ESP ne permet intentionnellement pas d'ICV de longueur zéro. C'est parce que GCM ne fournit aucune protection de l'intégrité lorsque utilisé avec une étiquette d'authentification de longueur zéro.

7. Expansion de paquet

La IV ajoute huit octets supplémentaires au paquet, et l'ICV encore 8, 12, ou 16 octets. Ce sont les seules sources d'expansion du paquet, autres que les 10 à 13 octets pris par les champs SPI ESP, Numéro de séquence, Bourrage, Longueur de bourrage, et Prochain en-tête (si la quantité minimale de bourrage est utilisée).

8. Conventions IKE

La présente section décrit les conventions utilisées pour générer le matériel de chiffrement et les valeurs de sel, à utiliser avec AES-GCM-ESP, en utilisant le protocole d'échange de clés Internet (IKE) [RFC2409]. Les identifiants et attributs nécessaires pour négocier une association de sécurité en utilisant AES-GCM-ESP sont aussi définis.

8.1 Matériel de chiffrement et valeurs de sel

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 un matériel de chiffrement de taille arbitraire, appelé KEYMAT. Le matériel de chiffrement est extrait de la chaîne de résultat sans égard aux frontières.

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

AES-GCM-ESP avec une clé de 128 bits
Le KEYMAT requis pour chaque clé AES-GCM fait 20 octets. Le 16 premiers octets sont la clé AES de 128 bits, et les quatre octets restants sont utilisés comme valeur de sel dans le nom occasionnel.

AES-GCM-ESP avec une clé de 192 bits
Le KEYMAT requis pour chaque clé AES-GCM fait 28 octets. Les 24 premiers octets sont les 192 bits de la clé AES, et les quatre octets restants sont utilisés comme valeur de sel dans le nom occasionnel.

AES-GCM-ESP avec une clé de 256 bits
Le KEYMAT requis pour chaque clé AES-GCM fait 36 octets. Les 32 premiers octets sont les 256 bits de la clé AES, et les quatre octets restants sont utilisés comme valeur de sel dans le nom occasionnel.

8.2 Identifiant de phase 1

Le présent document ne spécifie pas les conventions d'utilisation de AES-GCM pour les négociations IKE de phase 1. Pour que AES-GCM soit utilisé de cette manière, une spécification distincte est nécessaire, et un identifiant d'algorithme de

chiffrement doit être alloué. Les mises en œuvre DEVRAIENT utiliser un chiffrement IKE de phase 1 qui soit au moins aussi fort que AES-GCM. L'utilisation de AES CBC [RFC3602] avec la même taille de clé qu'utilisée par AES-GCM-ESP est RECOMMANDÉE.

8.3 Identifiant de phase 2

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

18 pour AES-GCM avec une ICV de 8 octets ;
19 pour AES-GCM avec une ICV de 12 octets ;
20 pour AES-GCM avec une ICV de 16 octets.

8.4 Attribut de longueur de clé

Parce que AES prend en charge trois longueurs de clés, 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.

9. Valeurs d'essai

L'Appendice B de [GCM] donne les valeurs d'essai qui vont aider ceux qui mettent en œuvre le mode AES-GCM.

10. Considérations sur la sécurité

GCM est d'une sûreté démontrable contre des adversaires qui peuvent choisir de façon adaptative les textes sources, les textes chiffrés, les ICV, et le champ AAD, sous des hypothèses cryptographiques standard (en gros, que le résultat du chiffrement sous-jacent, avec une clé choisie de façon aléatoire, ne peut pas être distingué d'un résultat choisi au hasard). Essentiellement, cela signifie que, si utilisé avec ses paramètres prévus, casser GCM implique de casser le chiffrement de bloc sous-jacent. La preuve de sécurité de GCM est disponible dans [GCM].

La considération de sécurité la plus importante est que la IV ne répète jamais une certaine clé. En partie, ceci est traité en interdisant l'utilisation de AES-GCM avec des clé configurées de façon statique, comme exposé à la Section 2.

Lorsque IKE est utilisé pour établir des clés fraîches entre deux entités homologues, des clés séparées sont établies pour les deux flux de trafic. Si on utilise un mécanisme différent pour établir des clés fraîches (qui établit seulement une simple 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 des collisions de bloc de compteur, les mises en œuvre 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 à l'association de sécurité des valeurs de sel différentes.

L'autre considération est que, comme avec tout mode de chiffrement, la sécurité de toutes les données protégées sous une certaine association de sécurité décroît légèrement avec chaque message.

Pour protéger contre ce problème, les mises en œuvre DOIVENT générer une clé fraîche avant de chiffrer 2^64 blocs de données avec une certaine clé. Noter qu'il est impossible d'atteindre cette limite en utilisant des numéros de séquence de 32 bits.

Noter que pour chaque message, GCM appelle le chiffrement de bloc une fois pour chaque bloc complet de 16 octets dans la charge utile, une fois pour chaque octet restant dans la charge utile, et une fois de plus pour calculer la ICV.

En clair, les plus petites valeurs d'ICV vont plus vraisemblablement être soumises à des attaques en contrefaçon. Les mises en œuvre DEVRAIENT utiliser une taille aussi grande que possible tout en restant raisonnable.

11. Raisons du concept

La présente spécification a été conçue comme étant un mécanisme aussi similaire que raisonnable à AES-CCM ESP [RFC4309] et AES-CTR ESP [RFC3686], tout en promouvant des mises en œuvre simples et efficaces à la fois dans les

matériels et les logiciels. On réutilise le concept et l'expérience de mise en œuvre de ces standard.

La différence majeure avec CCM est que le mécanisme CCM ESP exige un nom occasionnel de 11 octets, tandis que le mécanisme GCM ESP exige d'utiliser un nom occasionnel de 12 octets. GCM est spécialement optimisé pour traiter efficacement le cas du nom occasionnel de 12 octets. Les noms occasionnels d'une autre longueur causeraient une complexité supplémentaire et des délais inutiles, en particulier dans les mises en œuvre dans le matériel. L'octet supplémentaire du nom occasionnel est utilisé pour augmenter la taille du sel.

12. Considérations relatives à l'IANA

L'IANA a alloué trois identifiants de transformation ESP pour AES-GCM avec une IV explicite de huit octets :
18 pour AES-GCM avec une ICV de 8 octets ;
19 pour AES-GCM avec une ICV de 12 octets ;
20 pour AES-GCM avec une ICV de 16 octets.

13. Remerciements

Le présent travail est modélisé d'après la transformation AES-CCM [RFC4309]] de Russ Housley's . Des portions du présent document sont directement copiées de ce travail. Merci à Russ de son soutien.

De plus, le mode de fonctionnement GCM a été à l'origine conçu comme une amélioration du mode compteur de Carter-Wegman (CWC, *Carter-Wegman Counter*) [CWC], le premier mode de chiffrement de bloc non encombré capable de supporter le chiffrement authentifié à grande vitesse.

14. Références normatives

[GCM] Dworkin, M. "Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC", NIST Special Publication 800-38D, novembre 2007.

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

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

[RFC2407] D. Piper, "Le domaine d'interprétation de sécurité IP de l'Internet pour ISAKMP", novembre 1998. *(Obsolète, voir* RFC4306)

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

15. Références pour information

[CWC] Kohno, T., Viega, J. and D. Whiting, "CWC: A high-performance conventional authenticated encryption mode", Fast Software Encryption. http://eprint.iacr.org/2003/106.pdf , février 2004.

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

[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.)*

[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.)*

Adresse des auteurs

John Viega
Secure Software, Inc.
4100 Lafayette Center Dr., Suite 100
Chantilly, VA 20151
US
téléphone : (703) 814 4402
mél : viega@securesoftware.com

David A. McGrew
Cisco Systems, Inc.
510 McCarthy Blvd.
Milpitas, CA 95035
téléphone : (408) 525 8651
mél : mcgrew@cisco.com
URI : http://www.mindspring.com/~dmcgrew/dam.htm

Déclaration complète de droits de reproduction

Remerciement
Le financement de la fonction d'édition des RFC est fourni par la Administrative Support Activity (IASA) de l'IETF