Groupe de travail Réseau
Request for Comments : 4494
Catégorie : Sur la voie de la normalisation
Traduction Claude Brière de L'Isle

JH. Song, University of Washington
R. Poovendran, University of Washington
J. Lee, Samsung Electronics
juin 2006

L'algorithme AES-CMAC-96 et son utilisation avec IPsec

Résumé
L'Institut national des normes et technologies (NIST, *National Institute of Standards and Technology*) a récemment spécifié le code d'authentification de message fondé sur le chiffrement (CMAC, *Cipher-based Message Authentication Code*), qui est équivalent à l'algorithme MAC1 CBC à une clé (OMAC1, *One-Key CBC-MAC1*) soumis par Iwata et Kurosawa. OMAC1 réduit efficacement la taille de clé du mode étendu de chaînage de bloc de chiffrement (XCBC, *Extended Cipher Block Chaining mode*). Le présent mémoire spécifie l'utilisation du mode CMAC sur les mécanismes d'authentification des protocoles d'encapsulation de charge utile de sécurité (ESP, *Encapsulating Security Payload*) et d'en-tête d'authentification (AH, *Authentication Header*) de IPsec. Ce nouvel algorithme est appelé AES-CMAC-96.

1. Introduction

L'Institut national des normes et technologies (NIST, *National Institute of Standards and Technology*) a récemment spécifié le code d'authentification de message fondé sur le chiffrement (CMAC, *Cipher-based Message Authentication Code*). CMAC [NIST-CMAC] est un code d'authentification de message qui se fonde sur un chiffrement de bloc à clés symétriques, comme la norme de chiffrement avancée [NIST-AES]. CMAC est équivalent au MAC1 CBC à une clé (OMAC1) soumis par Iwata et Kurosawa [OMAC1a], [OMAC1b]. OMAC1 est une amélioration du mode de chaînage de bloc de chiffrement étendu (XCBC, *eXtended Cipher Block Chaining*) soumis par Black et Rogaway [XCBCa], [XCBCb], qui lui-même est une amélioration du code d'authentification de message à chaînage de bloc de chiffrement (CBC-MAC, *Cipher Block Chaining-Message Authentication Code)* de base. XCBC traite efficacement les déficiences de sécurité de CBC-MAC, et OMAC1 réduit efficacement la taille de clé de XCBC.

Le présent mémoire spécifie l'usage de CMAC sur le mécanisme d'authentification des protocoles d'encapsulation de charge utile de sécurité (ESP, *Encapsulating Security Payload*) [RFC4303] et d'en-tête d'authentification (AH, *Authentication Header*) [RFC4302] de IPsec. Ce nouvel algorithme s'appelle AES-CMAC-96. Pour plus d'informations sur AH et ESP, voir [RFC4302] et [RFC2411].

2. Définitions de base

CBC *(Cipher Block Chaining)* chaînage de bloc de chiffrement : mode de fonctionnement de pour le code d'authentification de message.

MAC *(Message Authentication Code)* code d'authentification de message. Chaîne binaire de longueur fixe, calculée par l'algorithme de génération de MAC, qui est utilisé pour établir l'autorité et donc, l'intégrité d'un message.

CMAC (Cipher-based MAC) MAC fondé sur le chiffrement. Il se fonde sur un chiffrement de bloc à clé symétrique approuvé, comme la norme de chiffrement avancée (AES, *Advanced Encryption Standard*).

Clé (K) : clé de 128 bits (16 octets) pour le bloc de chiffrement AES-128. Notée K.

Message (M) : le message à authentifier. Noté M.

Longueur (len) : longueur du message M en octets. Notée len. La valeur minimum est 0. La valeur maximum n'est pas spécifiée dans ce document.

tronquer(T,l) : tronquer T (MAC) dans l'ordre du bit de poids fort en premier (MSB-first) à une longueur de l octet.

T : le résultat de AES-CMAC.

T tronqué: résultat tronqué de AES-CMAC-128 dans l'ordre MSB en premier.

AES-CMAC : fonction de génération de CMAC fondés sur le chiffrement de bloc AES avec une clé de 128 bits.

AES-CMAC-96 : fonction de génération de MAC IPsec AH et ESP fondée sur AES-CMAC, qui tronque aux 96 bits de poids fort le résultat de 128 bits.

3. AES-CMAC

Le cœur de AES-CMAC-96 est l'AES-CMAC [RFC4493]. Les algorithmes sous-jacents pour AES-CMAC sont le bloc de chiffrement de la norme de chiffrement évolué [NIST-AES] et le mode de fonctionnement récemment défini CMAC [NIST-CMAC]. AES-CMAC donne une plus forte assurance d'intégrité des données qu'une somme de contrôle ou un code de détection d'erreur. La vérification d'une somme de contrôle ou d'un code de détection d'erreur détecte seulement des modifications accidentelles des données, tandis que CMAC est destiné à détecter les modifications intentionnelles non autorisées des données, ainsi que les modifications accidentelles. Le résultat de AES-CMAC peut valider le message d'entrée. Valider le message donne l'assurance de l'intégrité et de l'authenticité sur le message depuis la source. Conformément à [NIST-CMAC], au moins 64 bits devraient être utilisés contre les attaques pour les deviner. AES-CMAC réalise des objectifs de sécurité similaires à ceux de HMAC [RFC2104]. Comme AES-CMAC se fonde sur un chiffrement de bloc à clés symétriques (AES), alors que HMAC se fonde sur une fonction de hachage (comme SHA-1) AES-CMAC est approprié pour des systèmes d'informations dans lesquels AES est plus directement disponible qu'une fonction de hachage. On trouvera des informations détaillées sur AES-CMAC dans la [RFC4493] et dans [NIST-CMAC].

4. AES-CMAC-96

Pour l'authentification de message IPsec sur AH et ESP, AES-CMAC-96 devrait être utilisé. AES-CMAC-96 est un AES-CMAC avec un résultat tronqué à 96 bits dans l'ordre des bits de poids fort en premier. Le résultat est un MAC de 96 bits qui va satisfaire la longueur d'authentificateur par défaut spécifiée dans la [RFC4302]. Le résultat de la troncature est pris dans l'ordre des bits de poids fort en premier. Pour plus d'informations sur AES-CMAC, voir la [RFC4493] et [NIST-CMAC].

La Figure 1 décrit l'algorithme AES-CMAC-96 :

Dans l'étape 1, AES-CMAC est appliqué au message M de longueur len avec la clé K.

Dans l'étape 2, le bloc de résultat T est tronqué à 12 octets dans l'ordre des bits de poids fort en premier, et T tronqué (TT) est retourné.

```
Entrées :   K (clé de 128 bits décrite au paragraphe 4.1)
            M (message à authentifier)
            len (longueur du message en octets)
Résultat : T tronqué (résultat tronqué à 12 octets)

Étape 1.  T  := AES-CMAC (K,M,len) ;
Étape 2.  TT := tronquer (T, 12) ;
          retourne TT ;
```

Figure 1 : Algorithme AES-CMAC-96

5. Vecteurs d'essai

Ces cas d'essai sont les mêmes que défini dans [NIST-CMAC], à l'exception de la troncature à 96 bits.

K 2b7e1516 28aed2a6 abf71588 09cf4f3c
Génération de sous clé
AES_128(key,0) 7df76b0c 1ab899b3 3e42f047 b91b546f
K1 fbeed618 35713366 7c85e08f 7236a8de
K2 f7ddac30 6ae266cc f90bc11e e46d513b

Cas d'essai 1 : len = 0
M <chaîne vide>
AES_CMAC_96 bb1d6929 e9593728 7fa37d12

Cas d'essai 2 : len = 16
M 6bc1bee2 2e409f96 e93d7e11 7393172a
AES_CMAC_96 070a16b4 6b4d4144 f79bdd9d

Cas d'essai 3 : len = 40
M 6bc1bee2 2e409f96 e93d7e11 7393172a ae2d8a57 1e03ac9c 9eb76fac 45af8e51 30c81c46 a35ce411
AES_CMAC_96 dfa66747 de9ae630 30ca3261

Cas d'essai 4 : len = 64
M 6bc1bee2 2e409f96 e93d7e11 7393172a ae2d8a57 1e03ac9c 9eb76fac 45af8e51
30c81c46 a35ce411 e5fbc119 1a0a52ef f69f2445 df4f9b17 ad2b417b e66c3710
AES_CMAC_96 51f0bebf 7e3b9d92 fc497417

6. Interaction avec le mécanisme de chiffrement ESP

Au moment de la rédaction du présent mémoire, aucun problème connu n'empêche l'utilisation de AES-CMAC-96 avec un algorithme de chiffrement spécifique.

7. Considérations sur la sécurité

Voir la Section Considérations sur la sécurité de la [RFC4493].

8. Considérations relatives à l'IANA

L'IANA a alloué la valeur 8 pour la transformation IKEv2 de type 3 (algorithme d'intégrité) à l'algorithme AUTH_AES_CMAC_96.

9. Remerciements

Des portions du texte présenté ici sont empruntées à [NIST-CMAC] et [XCBCa]. On remercie Russ Housley de ses utiles commentaires.

On remercie de leur soutien les organismes suivants : Collaborative Technology Alliance (CTA) du US Army Research Laboratory, DAAD19- 01-2-0011 ; Presidential Award du Army Research Office, W911NF-05-1-0491; NSF CAREER ANI-0093187. Les résultats ne reflètent pas nécessairement la position de ces agences de financement.

10. Références

10.1 Références normatives

[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.)*

[RFC4493] JH. Song et autres, "Algorithme AES-CMAC", juin 2006. *(Information)*

[NIST-AES] NIST, FIPS 197, "Advanced Encryption Standard (AES)", novembre 2001. http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

[NIST-CMAC] NIST, Special Publication 800-38B, "Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication", mai 2005.

10.2 Références pour information

[OMAC1a] Tetsu Iwata and Kaoru Kurosawa, "OMAC: One-Key CBC MAC", Fast Software Encryption, FSE 2003, LNCS 2887, pp. 129-153, Springer-Verlag, 2003.

[OMAC1b] Tetsu Iwata and Kaoru Kurosawa, "OMAC: One-Key CBC MAC", Submission to NIST, décembre 2002. Disponible à http://csrc.nist.gov/CryptoToolkit/modes/proposedmodes/omac/omac-spec.pdf

[RFC2104] H. Krawczyk, M. Bellare et R. Canetti, "HMAC : Hachage de clés pour l'authentification de message", février 1997.

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

[XCBCa] John Black and Phillip Rogaway, "A Suggestion for Handling Arbitrary-Length Messages with the CBC MAC", NIST Second Modes of Operation Workshop, août 2001. Disponible à http://csrc.nist.gov/CryptoToolkit/modes/proposedmodes/xcbc-mac/xcbc-mac-spec.pdf

[XCBCb] John Black and Phillip Rogaway, "CBC MACs for Arbitrary-Length Messages: The Three-Key Constructions", Journal of Cryptology, Vol. 18, No. 2, pp. 111-132, Springer-Verlag, Spring 2005.

Adresse des auteurs

Junhyuk Song
University of Washington
Samsung Electronics
USA
téléphone : (206) 853-5843
mél : junhyuk.song@samsung.com

Jicheol Lee
Samsung Electronics
téléphone : +82-31-279-3605
mél : jicheol.lee@samsung.com

Radha Poovendran
Network Security Lab
University of Washington
USA
téléphone : (206) 221-6512
mél : radha@ee.washington.edu

Déclaration complète de droits de reproduction

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 faites 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 assuré par la Internet Society.