Groupe de travail Réseau
Request for Comments : 4434
RFC rendue obsolète : 3664
Catégorie: Sur la voie de la normalisation

P. Hoffman, VPN Consortium
février 2006

Traduction Claude Brière de L'Isle

Algorithme AES-XCBC-PRF-128 pour le protocole d'échange de clé Internet (IKE)

Résumé
Certaines mises en œuvre de la sécurité IP (IPsec) peuvent vouloir utiliser une fonction pseudo aléatoire dérivée de la norme de chiffrement évoluée (AES, *Advanced Encryption Standard*). Le présent document décrit un tel algorithme, appelé AES-XCBC-PRF-128.

1. Introduction

La [RFC3566] décrit une méthode pour utiliser la norme de chiffrement évolué (AES, *Advanced Encryption Standard*) comme un code d'authentification de message (MAC, *Message Authentication Code*) dont le résultat fait 96 bits. Bien que 96 bits soient considérés comme appropriés pour un MAC, c'est trop court pour être utile comme fonction pseudo aléatoire (PRF, *pseudo-random function*) de longue durée dans IKE version 1 ou version 2. Les deux versions de IKE utilisent la PRF pour créer des clés d'une façon qui dépend de la longueur du résultat de la PRF. Utiliser une PRF qui a un résultat de 96 bits crée des clés qui sont plus faciles à attaquer en force brute qu'une PRF qui utilise un résultat de 128 bits.

Heureusement, il y a une méthode très simple pour utiliser la plus grande partie de AES-XCBC-PRF comme une PRF dont le résultat est 128 bits : omettre l'étape qui tronque la valeur de 128 bits à 96 bits.

1.1 Différences avec la RFC 3664

Le présent document spécifie le même algorithme que la RFC 3664 sauf qu'est supprimée la restriction de la [RFC3566] que les clés soient exactement de 128 bits. Les mises en œuvre de la RFC 3664 auront le même résultat de bits dans le réseau que cet algorithme ; la seule différence est que les clés qui n'étaient pas égales en longueur à 128 bits ne seront plus rejetées mais seront alignées sur 128 bits.

IKEv2 [RFC4306] utilise des PRF pour plusieurs objets, principalement pour générer du matériel de chiffrement et d'authentification de la IKE_SA. La spécification IKEv2 fait une différence entre les PRF avec des tailles de clé fixe et celles qui ont des tailles de clé variables.

Quand la PRF décrite dans le présent document est utilisée avec IKEv2, la PRF est considérée être de longueur fixe pour générer le matériel de chiffrement, mais de longueur variable pour l'authentification. C'est-à-dire que quand on génère le matériel de chiffrement, "la moitié des bits doit venir de Ni et la moitié de Nr, en prenant les premiers bits de chaque" comme décrit dans IKEv2, paragraphe 2.14 ; mais pour l'authentification avec des secrets partagés (IKEv2, paragraphe 2.16) le secret partagé n'a pas à être long de 128 bits. Cette logique un peu torturée permet aux mises en œuvre de IKEv2 qui utilisent la sémantique de clé de longueur fixe de la RFC 3664 d'interopérer avec les mises en œuvre qui utilisent la sémantique de clé de longueur variable du présent document.

2. Algorithme AES-XCBC-PRF-128

L'algorithme AES-XCBC-PRF-128 est identique à celui de la [RFC3566] excepté deux changements. D'abord, la restriction de la longueur de clé de exactement 128 bits de la [RFC3566] est éliminée, comme décrit ci-dessous ; cela aligne AES-XCBC-PRF-128 sur HMAC-SHA1 et HMAC-MD5 quand ils sont utilisés comme PRF dans IKE. Ensuite, l'étape de troncature du paragraphe 4.3 de la [RFC3566] *n'est pas* effectuée ; c'est-à-dire, il n'y a pas de traitement après le paragraphe 4.2 de la [RFC3566].

La clé pour AES-XCBC-PRF-128 est créée comme suit :

- Si la clé fait exactement 128 bits, on l'utilise comme elle est.
- Si la clé fait moins de 128 bits, on l'allonge à exactement 128 bits en la bourrant à droite de bits à zéro.
- Si la clé fait 129 bits ou plus, on la raccourcit à exactement 128 bits en effectuant les étapes de AES-XCBC-PRF-128 (c'est-à-dire, l'algorithme décrit dans le présent document). Dans cette ré-application de cet algorithme, la clé est de 128 bits à zéro ; le message est la clé courante trop longue.

2.1 Vecteurs d'essai

Cas d'essai AES-XCBC-PRF-128 avec entrée de 20 octets
Clé : 000102030405060708090a0b0c0d0e0f
Longueur de clé : 16
Message : 000102030405060708090a0b0c0d0e0f10111213
Résultat de la PRF : 47f51b4564966215b8985c63055ed308

Cas d'essai AES-XCBC-PRF-128 avec entrée de 20 octets
Clé : 00010203040506070809
Longueur de clé : 10
Message : 000102030405060708090a0b0c0d0e0f10111213
Résultat de la PRF : 0fa087af7d866e7653434e602fdde835

Cas d'essai AES-XCBC-PRF-128 avec entrée de 20 octets
Clé : 000102030405060708090a0b0c0d0e0fedcb
Longueur de clé : 18
Message : 000102030405060708090a0b0c0d0e0f10111213
Résultat de la PRF : 8cd3c93ae598a9803006ffb67c40e9e4

3. Considérations sur la sécurité

La sécurité fournie par AES-XCBC-MAC-PRF se fonde sur la force de AES et de HMAC. Au moment de cette rédaction, il n'y a pas d'attaque cryptographique pratique connue contre AES, AES-XCBC-MAC-PRF, ou HMAC.

Comme il est vrai de tout algorithme de chiffrement, une partie de sa force repose dans la sécurité du mécanisme de gestion de clé, dans la force de la clé secrète associée, et dans la correction des mises en œuvre de tous les systèmes participants. La [RFC3566] contient des vecteurs d'essai pour aider à la vérification de la correction du code AES-XCBC-MAC-PRF. Les vecteurs d'essai montrent tous la valeur complète du MAC avant sa troncature à 96 bits. La PRF utilise la valeur de MAC complète, pas celle qui est tronquée.

4. Considérations relatives à l'IANA

Toutes les références à la RFC 3664 doivent être mises à jour pour se référer au présent document quand il sera publié.

5. Références normatives

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

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

6. Remerciements

Pasi Eronen a suggéré la méthode pour raccourcir es clés trop longues. Saroop Mathur et John Black ont fourni et vérifié les vecteurs d'essai.

Adresse de l'auteur

Paul Hoffman
VPN Consortium

mél : paul.hoffman@vpnc.org

Déclaration complète de droits de reproduction

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