Groupe de travail Réseau
Request for Comments : 4615
Catégorie : Standards Track
Août 2006

J. Song
R. Poovendran, University of Washington
J. Lee, Samsung Electronics
T. Iwata, Nagoya University
Traduction Claude Brière de L'Isle

Algorithme évolué de la fonction 128 de code pseudo-aléatoire d'authentification de message fondée sur le chiffrement standard (AES-CMAC-128) pour le protocole d'échange de clés sur Internet (IKE)

Statut de ce mémo

Le présent document spécifie un protocole de normalisation Internet pour la communauté de l'Internet, qui appelle à la discussion et à des suggestions pour son amélioration. Prière de se reporter à l'édition en cours des "Normes de protocole officielles de l'Internet" (STD 1) sur l'état de la normalisation et le statut de ce protocole. La distribution du présent mémo n'est soumise à aucune restriction.

Notice de Copyright

Résumé

Certaines mises en œuvre de sécurité sur IP (IPsec) peuvent vouloir utiliser une fonction pseudo-aléatoire (PRF, *pseudo-random function*) fondée sur la norme de codage évolué (AES, *Advanced Encryption Standard*). Le présent mémo décrit un tel algorithme, sous le nom de AES-CMAC-PRF-128. Il prend en charge des tailles de clé fixes et variables.

Table des matières

1 Introduction

La [RFC4493] décrit une méthode d'utilisation de la norme de codage évolué (AES) comme code d'authentification de message (MAC, *Message Authentication Code*) qui a une longueur de sortie de 128 bits. La sortie de 128 bits est utile comme fonction pseudo aléatoire (PRF, *pseudo-random function*) de longue durée. Le présent document spécifie une PRF qui prend en charge des tailles de clé fixes et variables pour la fonction de déduction de clé (KDF, *Key Derivation Function*) et l'authentification IKEv2 [RFC4306].

2 Définitions de base

VK	Clé de longueur variable pour AES-CMAC-PRF-128, notée VK.
0^128	Chaîne comportant 128 bits zéro, qui est équivalente à 0x00000000000000000000000000000000 en notation hexadéecimale.
AES-CMAC	Algorithme AES-CMAC avec une clé longue de 128 bits décrite au paragraphe 2.4 de la [RFC4493].

3 Algorithme AES-CMAC-PRF-128

L'algorithme AES-CMAC-PRF-128 est identique au AES-CMAC défini dans la [RFC4493] excepté que la restriction sur la longueur de clé de 128 bits est supprimée.

IKEv2 [RFC4306] utilise les PRF pour des besoins multiples, dont le plus notable est de générer du matériel de calcul de clés et d'authentification du IKE_SA. La spécification IKEv2 différencie les PRF avec taille de clé fixe et ceux qui ont des tailles de clé variables.

Lors de l'utilisation de AES-CMAC-PRF-128 comme PRF tel que décrit dans IKEv2, AES-CMAC-PRF-128 est censé prendre des clés de taille fixe (16 octets) pour générer le matériel de calcul de clés mais il prend des clés de taille variable pour l'authentification.

C'est-à-dire que lors de la génération du matériel de calcul de clé, "la moitié des bits doivent venir de Ni et la moitié de Nr, en prenant les premiers bits de chacun" comme décrit au paragraphe 2.14 de IKEv2 ; mais pour l'authentification avec secrets partagés (IKEv2, paragraphe 2.16), le secret partagé n'a pas obligatoirement 16 octets et sa longueur peut varier.

AES-CMAC-PRF-128		
Entrée :	VK	(Clé de longueur variable)
	M	(Message, c'est-à-dire, les données d'entrée de la PRF)
	VKlen	(longueur de VK en octets)
	len	(longueur de M en octets)
Sortie :	PRV	(Variable pseudo-aléatoire de 128 bits)
	Variable:	K (clé de 128-bit pour AES-CMAC)
	étape 1.	si VKlen est égal à 16
	étape 1a.	alors
		K := VK;
	étape 1b.	autrement
		K := AES-CMAC(0^128, VK, VKlen);
	étape 2. ;	PRV := AES-CMAC(K, M, len)
		retour PRV ;

Figure 1. Algorithme AES-CMAC-PRF-128

À l'étape 1, la clé de 128-bit, K, pour AES-CMAC est déduite comme suit :

Si la clé, VK, est exactement de 128 bits, on l'utilise alors comme elle est.

Si elle est plus longue ou plus courte que 128 bits, on déduit alors la clé, K, en appliquant l'algorithme AES-CMAC en utilisant la chaîne de 128 bits tous à zéro comme clé et VK comme le message d'entrée. Cette étape est décrite en 1b.

À l'étape 2, on applique l'algorithme AES-CMAC en utilisant K comme clé et M comme message d'entrée. Le résultat de l'algorithme est le retour.

4 Vecteurs d'essai

Cas d'essai AES-CMAC-PRF-128 avec une entrée de 20 octets
Clé : 00010203 04050607 08090a0b 0c0d0e0f edcb
Longueur de clé : 18
Message : 00010203 04050607 08090a0b 0c0d0e0f 10111213
Sortie PRF : 84a348a4 a45d235b abfffc0d 2b4da09a

Cas d'essai AES-CMAC-PRF-128 avec une entrée de 20 octets
Clé : 00010203 04050607 08090a0b 0c0d0e0f
Longueur de clé : 16
Message : 00010203 04050607 08090a0b 0c0d0e0f 10111213
Sortie PRF : 980ae87b 5f4c9c52 14f5b6a8 455e4c2d

Cas d'essai AES-CMAC-PRF-128 avec une entrée de 20 octets
Clé : 00010203 04050607 0809
Longueur de clé : 10
Message : 00010203 04050607 08090a0b 0c0d0e0f 10111213
Sortie PRF : 290d9e11 2edb09ee 141fcf64 c0b72f3d

5 Considérations de sécurité

La sécurité fournie par AES-CMAC-PRF-128 se fonde sur la force d'AES et d'AES-CMAC. Au moment où ce document est écrit, aucune attaque cryptographique pratique contre AES ou AES-CMAC n'est connue. Cependant, comme il en va avec tout algorithme cryptographique, une part de sa force réside dans la clé secrète, VK, et dans la correction des mises en œuvre dans tous les systèmes participants. La clé, VK, doit être choisie de façon indépendante et aléatoire sur la base de la RFC 4086 [RFC4086], et les deux clés, VK et K, devraient être conservées en sûreté et rafraîchies périodiquement. La Section 4 présente des vecteurs d'essai qui aident à la vérification de la correction du code AES-CMAC-PRF-128.

Si VK est plus long que 128 bits et est raccourci pour satisfaire à la taille de clé de AES-128, une certaine entropie peut être perdue. Cependant, tant que VK est plus long que 128 bits, la nouvelle clé, K, préserve une entropie suffisante, c'est-à-dire que l'entropie de K est d'environ128 bits.

On recommande donc l'utilisation d'un VK supérieur ou égal à 128 bits, et on déconseille l'utilisation d'un VK inférieur ou égal à 64 bits, à cause de la faible entropie.

6 Considérations relatives à l'IANA

IANA a alloué une valeur de 8 pour la transformée de type de d'IKEv2 (fonction pseudo-aléatoire) à l'algorithme PRF_AES128_CMAC.

7 Remerciements

Certaines portions du présent texte ont été empruntées à la [RFC3664] et à la [RFC4434]. Tous nos remerciements à Russ Housley et Paul Hoffman pour leurs suggestions et leurs conseils. Nous remercions aussi Alfred Hoenes pour ses nombreux commentaires utiles.

Nous remercions de leur soutien leur contributeurs suivants : Collaborative Technology Alliance (CTA) de l'US Army Research Laboratory, DAAD19-01-2-0011 ; Presidential Award de l'Army Research Office,-W911NF-05-1-0491 ; ONR YIP N00014-04-1-0479. Les résultats ne reflètent aucune position des agences de financement.

8 Références

8.1 Références normatives

[RFC4493] Song, JH., Poovendran, R., Lee, J., et T. Iwata, "L'algorithme AES-CMAC", RFC 4493, juin 2006.

[RFC4306] Kaufman, C., "Protocle d'échange de clé sur Internet (IKEv2)", RFC 4306, décembre 2005.

[RFC4086] Eastlake, D., 3rd, Schiller, J., et S. Crocker, "Exigences d'aléa pour la sécurité", BCP 106, RFC 4086, juin 2005.

8.2 Références informatives

[RFC3664] Hoffman, P., "L'algorithme AES-XCBC-PRF-128 pour le protocole d'échange de clés sur Internet (IKE)", RFC 3664, janvier 2004.

[RFC4434] Hoffman, P., "L'algorithme AES-XCBC-PRF-128 pour le protocole d'échange de clés sur Internet (IKE)", RFC 4434, février 2006.

Adresses des auteurs

JunHyuk Song	Radha Poovendran
Samsung Electronics	Network Security Lab
University of Washington	University of Washington
Phone: (206) 853-5843	Phone: (206) 221-6512
EMail: junhyuk.song@samsung.com	EMail: radha@ee.washington.edu
junhyuk.song@gmail.com	Radha Poovendran

Jicheol Lee	Tetsu Iwata
Samsung Electronics	Nagoya University
Phone: +82-31-279-3605	
EMail: jicheol.lee@samsung.com	EMail: iwata@cse.nagoya-u.ac.jp

Déclaration de copyright

Propriété intellectuelle

Remerciement

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