Groupe de travail Réseau
Request for Comments: 5529
Catégorie : Sur la voie de la normalisation
Traduction Claude Brière de L'Isle

A. Kato, NTT Software Corporation
M. Kanda, NTT
S. Kanno, NTT Software Corporation
avril 2009

Modes de fonctionnement pour Camellia avec IPsec

Résumé
Le présent document décrit l'utilisation de l'algorithme de chiffrement de bloc Camellia en mode de chaînage de bloc de chiffrement (CBC, *Cipher Block Chaining*) en mode Compteur (CTR, *Counter*) et en mode Compteur avec CBC-MAC (CCM, *Counter with CBC-MAC*) comme mécanismes supplémentaires de mise en œuvre facultative du protocole d'échange de clé Internet version 2 (IKEv2, *Internet Key Exchange Protocol version 2*) et d'encapsulation de charge utile de sécurité (ESP, *Encapsulating Security Payload*) pour assurer la confidentialité, l'authentification de l'origine des données, et l'intégrité sans connexion.

Table des matières

1. Introduction

Le présent document décrit l'utilisation de l'algorithme de chiffrement de bloc Camellia [RFC3713] en mode de chaînage de bloc de chiffrement (CBC, *Cipher Block Chaining*) en mode Compteur (CTR) et en mode Compteur avec CBC-MAC (CCM, *CBC-MAC*) comme mécanismes supplémentaires de mise en œuvre facultative de IKEv2 [RFC4306] et de l'encapsulation de charge utile de sécurité (ESP, *Encapsulating Security Payload*) [RFC4303] pour fournir la confidentialité, l'authentification de l'origine des données, et l'intégrité sans connexion.

Comme le code de source optimisé est fourni sous plusieurs licenses gratuites [SOURCE], Camellia est aussi adopté par plusieurs projets en source ouverte (OpenSSL, FreeBSD Linux, et Firefox Gran Paradiso).

La spécification de l'algorithme et les identifiants d'objet sont décrits dans la [RFC3713].

Le site de la Toile de Camellia [WEB] contient une quantité d'informations sur Camellia, incluant une spécification détaillée, une analyse de la sécurité, des chiffres de performances, des mises en œuvre de référence, des mises en œuvre optimisées, des vecteurs d'essai, et des informations de propriété intellectuelle.

Le reste de ce document spécifie l'utilisation de divers modes de fonctionnement pour Camellia dans le contexte de IPsec ESP. Pour d'autres informations sur la façon dont les diverses pièces de IPsec en général et de ESP en particulier s'assemblent pour fournir des services de sécurité, se référer aux [RFC4301] et [RFC4303].

1.1 Terminologie

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. Algorithme de chiffrement Camellia

Tous les algorithmes de chiffrement de bloc symétrique partagent des caractéristiques et variables communes, incluant le mode, la taille de clés, les clés faibles, la taille de bloc, et les tours. Les caractéristiques pertinentes de Camellia sont décrites dans la [RFC3713].

2.1 Taille et bourrage de bloc

Camellia utilise une taille de bloc de 16 octets (128 bits).

Les exigences de bourrage sont décrites dans :
(a) Exigences de bourrage pour Camellia [RFC4303],
(b) Exigences de bourrage pour Camellia-CBC [RFC4303],
(c) Exigences de bourrage pour Camellia-CCM [NIST],
(d) Exigences de bourrage pour ESP [RFC4303].

2.2 Performances

Les chiffres de performances pour Camellia sont disponibles dans [WEB]. Le projet NESSIE a fait un rapport sur les performances de mises en œuvre optimisées indépendantes [NESSIE].

3. Modes

Le présent document décrit trois modes de fonctionnement pour l'utilisation de Camellia avec IPsec : chaînage de bloc de chiffrement (CBC, *Cipher Block Chaining*), Compteur (CTR, *Counter*), et Compteur avec CBC-MAC (CCM, *Counter with CBC-MAC*).

3.1 Chaînage de bloc de chiffrement

Le mode CBC de Camellia est défini dans la [RFC4312].

3.2 Compteur et compteur avec CBC-MAC

Camellia dans les modes CTR et CCM est utilisé dans IPsec comme AES dans les [RFC4309] et [RFC3686]. Dans la présente spécification, CCM est utilisé avec le bloc de chiffrement de bloc Camellia [RFC5528].

4. Conventions IKEv2

Cette section décrit l'identifiant de transformation et les conventions utilisées pour générer le matériel de chiffrement à utiliser avec ENCR_CAMELLIA_CBC, ENCR_CAMELLIA_CTR, et ENCR_CAMELLIA_CCM en utilisant l'échange de clés Internet (IKEv2) [RFC4306].

4.1 Matériel de chiffrement

La taille de KEYMAT DOIT être égale ou supérieure à la clé Camellia associée. Le matériel de chiffrement est utilisé comme suit :

Camellia-CBC avec une clé de 128 bits ; la KEYMAT demandée pour chaque clé Camellia-CBC fait 16 octets. Tous les 16 octets sont la clé Camellia de 128 bits.

Camellia-CBC avec une clé de 192 bits : la KEYMAT demandée pour chaque clé Camellia-CBC fait 24 octets. Tous les 24 octets sont la clé Camellia de 192 bits.

Camellia-CBC avec une clé de 256 bits : la KEYMAT demandée pour chaque clé Camellia-CBC fait 32 octets. Tous les 32 octets sont la clé Camellia de 256 bits.

Camellia-CTR avec une clé de 128 bits :la KEYMAT demandée pour chaque clé Camellia-CTR fait 20 octets. Les 16 premiers octets sont la clé Camellia de 128 bits, et les quatre octets restants sont utilisés comme valeur de nom occasionnel dans le bloc compteur.

Camellia-CTR avec une clé de 192 bits : la KEYMAT demandée pour chaque clé Camellia-CTR fait 28 octets. Les 24 premiers octets sont la clé Camellia de 192 bits, et les quatre octets restants sont utilisés comme valeur de nom occasionnel dans le bloc compteur.

Camellia-CTR avec une clé de 256 bits : la KEYMAT demandée pour chaque clé Camellia-CTR fait 36 octets. Les 32 premiers octets sont la clé Camellia de 256 bits, et les quatre octets restants sont utilisés comme valeur de nom occasionnel dans le bloc compteur.

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

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

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

4.2 Transformation de type 1

Pour les négociations IKEv2, l'IANA a alloué cinq identifiants de transformation ESP pour Camellia-CBC, Camellia-CTR, et Camellia-CCM, comme indiqué à la Section 6.

4.3 Attribut Longueur de clé

Comme Camellia supporte trois longueurs de clé, l'attribut Longueur de clé DOIT être spécifié dans l'échange IKE [RFC4306]. L'attribut longueur de clé DOIT avoir une valeur de 128, 192, ou 256 bits.

5. Considérations sur la sécurité

Pour les questions de sécurité des modes CTR et CCM, le présent document se réfère à la Section 9 de la [RFC4309] et à la

Section 7 de la [RFC3686].

Aucun problème de sécurité n'a été trouvé pour Camellia [IPA], [NESSIE].

6. Considérations relatives à l'IANA

L'IANA a alloué des paramètres IKEv2 à utiliser avec Camellia-CTR et avec Camellia-CCM pour le type de transformation 1 (algorithme de chiffrement) :

23 pour ENCR_CAMELLIA_CBC ;
24 pour ENCR_CAMELLIA_CTR ;
25 pour ENCR_CAMELLIA_CCM avec un ICV de 8 octets ;
26 pour ENCR_CAMELLIA_CCM avec un ICV de 12 octets ;
27 pour ENCR_CAMELLIA_CCM avec un ICV de 16 octets.

7. Remerciements

Merci à Tim Polk et Tero Kivinen de leur relecture initiale de ce document. Merci à Derek Atkins et Rui Hodai de leurs commentaires et suggestions. Un merci particulier à Alfred Hoenes pour ses relectures très détaillées et ses suggestions.

8. Références

8.1 Références normatives

[NIST] Dworkin, M., "Recommendation for Block Cipher Modes of Operation: the CCM Mode for Authentication and Confidentiality", NIST Special Publication 800-38C, juillet 2007, <http://csrc.nist.gov/publications/nistpubs/800-38C/SP800-38C_updated-July20_2007.pdf>.

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

[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.)*

[RFC3713] M. Matsui, J. Nakajima, S. Moriai, "Description de l'algorithme de chiffrement Camellia", avril 2004. *(Information)*

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

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

[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.)*

[RFC4312] A. Kato et autres, "L'algorithme de chiffrement Camellia et son utilisation avec IPsec", décembre 2005. *(P.S.)*

8.2 Références pour information

[IPA] Information-technology Promotion Agency (IPA), "Cryptography Research and Evaluation Committees", <http://www.ipa.go.jp/security/enc/CRYPTREC/index-e.html>.

[NESSIE] "The NESSIE project (New European Schemes for Signatures, Integrity and Encryption)",

<http://www.cosic.esat.kuleuven.be/nessie/>.

[RFC4301] S. Kent et K. Seo, "Architecture de sécurité pour le protocole Internet", DOI 10.17487/RFC4301, décembre 2005. *(P.S.) (Remplace la* RFC2401)

[RFC5528] A. Kato, M. Kanda, S. Kanno, "Mode compteur Camellia et compteur Camellia avec les algorithmes de mode CBC-MAC" avril 2009. *(Information)*

[SOURCE] "Camellia open source software", <http://info.isl.ntt.co.jp/crypt/eng/camellia/source.html>.

[WEB] "Camellia web site", <http://info.isl.ntt.co.jp/camellia/>.

Adresse des auteurs

Akihiro Kato
NTT Software Corporation
mél : akato@po.ntts.co.jp

Masayuki Kanda
NTT
mél : kanda.masayuki@lab.ntt.co.jp

Satoru Kanno
NTT Software Corporation
mél : kanno-s@po.ntts.co.jp