Groupe de travail Réseau
Request for Comments : 4312
Catégorie : Sur la voie de la normalisation
Traduction Claude Brière de L'Isle

A. Kato, NTT Software Corporation
S. Moriai, Sony Computer Entertainment Inc.
M. Kanda, Nippon Telegraph and Telephone Corporation
décembre 2005

Utilisation de l'algorithme de chiffrement 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, avec une valeur d'initialisation explicite, comme mécanisme de confidentialité dans le contexte de l'encapsulation de charge utile de sécurité IPsec (ESP).

1. Introduction

Le présent document décrit l'utilisation de l'algorithme de chiffrement de bloc Camellia en mode de chaînage de bloc de chiffrement, avec une valeur explicite d'initialisation, comme mécanisme de confidentialité dans le contexte de l'encapsulation de charge utile de sécurité (ESP, *Encapsulating Security Payload*) d'IPsec.

Camellia a été choisi comme primitive cryptographique recommandée par le projet NESSIE (Nouveaux schémas européens pour les signatures, l'intégrité et le chiffrement) [NESSIE] de l'Union Européenne et a été inclus dans la liste des techniques cryptographiques pour les systèmes japonnais de gestion électronique choisies par le comité CRYPTREC (*Cryptography Research, Evaluation Committees*) [CRYPTREC] du Japon. Camellia a été soumis à plusieurs autres organisations de normalisation, comme l'ISO (ISO/CEI 18033) et le groupe de travail Sécurité de la messagerie électronique [RFC3657] de l'IETF.

Camellia accepte des tailles de bloc de 128 bits et des longueurs de clé de 128, 192, et 256 bits, c'est-à-dire, les mêmes spécifications d'interface que la norme de chiffrement évolué (AES, *Advanced Encryption Standard*) [AES].

Camellia est un chiffrement symétrique avec une structure de Feistel. Camellia a été développé conjointement par NTT et la Mitsubishi Electric Corporation en 2000. Il été conçu pour résister à toutes les attaques de cryptanalyse connues, et il a été examiné par les experts en cryptographie du monde entier. Camellia convient pour une mise en œuvre de logiciel et de matériel, offrant une vitesse de chiffrement dans les mises en œuvre de logiciels et matériels comparable à celle de AES.

La page d'accueil de Camellia [Camellia-Web] contient de nombreuses informations sur Camellia, incluant sa spécification détaillée, l'analyse de sa sécurité, des chiffres de performances, des références de mise en œuvre, des vecteurs d'essai, et des informations de propriété intellectuelle.

Le reste de ce document spécifie l'utilisation de Camellia dans le contexte de IPsec ESP. Pour plus d'informations sur la façon dont les diverses pièces de ESP s'assemblent pour fournir des services de sécurité, se référer aux [RFC2401], [RFC2411], et [RFC4303].

1.1 Spécification des exigences

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 symétriques partagent des caractéristiques et variables communes, incluant le mode, la taille de clé, les clés faibles, la taille de bloc, et des tours. Les paragraphes qui suivent contiennent la description des caractéristiques pertinentes de Camellia.

La spécification de l'algorithme et des identifiants d'objets figure dans la [RFC3713].

2.1 Mode

Le NIST a défini cinq modes de fonctionnement pour AES et autres chiffrements approuvés par FIPS [SP800-38a] : CBC (*Cipher Block Chaining*, chaînage de bloc de chiffrement), ECB (*Electronic CodeBook*, livre de code électronique), CFB (*Cipher FeedBack*, chiffrement avec retour), OFB (*Output FeedBack*, retour sur résultat), et CTR (Compteur). Le mode CBC est bien défini et bien compris pour les chiffrements symétriques, et il est actuellement exigé pour tous les autres chiffrements d'ESP. Le présent document spécifie l'utilisation du chiffrement Camellia en mode CBC au sein de ESP. Ce mode exige une taille de valeur d'initialisation (IV) qui soit la même que la taille de bloc. L'utilisation d'une IV générée de façon aléatoire empêche la génération d'un texte chiffré identique à partir de paquets qui ont des données identiques s'étendant sur le premier bloc de la taille de bloc de l'algorithme de chiffrement.

L'IV CBC est OUXée avec le premier bloc de texte source avant qu'il soit chiffré. Ensuite, pour les blocs suivants, le bloc de texte chiffré précédent est OUXé avec le texte source courant avant qu'il soit chiffré. Plus d'informations sur le mode CBC peuvent être obtenues dans [SP800-38a], [CRYPTO-S].

2.2 Taille de clé

Camellia prend en charge trois tailles de clés : 128 bits, 192 bits, et 256 bits. La taille de clé par défaut est 128 bits, et toutes les mises en œuvre DOIVENT prendre en charge cette taille de clé. Les mises en œuvre PEUVENT aussi prendre en charge des tailles de clé de 192 bits et 256 bits.

Camellia utilise un nombre de tours différent pour chacun des tailles de clé définie. Quand on utilise une taille de clé de 128 bits, la mise en œuvre DOIT utiliser 18 tours. Quand on utilise une clé de 192 bits, la mise en œuvre DOIT utiliser 24 tours. Avec une clé de 256 bits, on DOIT utiliser 24 tours.

2.3 Clé faibles

Au moment de la rédaction du présent document, il n'y a pas de clé faible connue pour Camellia.

2.4 Taille de bloc et bourrage

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

Un bourrage est requis par les algorithmes pour maintenir une taille de bloc de 16 octets (128 bits). Le bourrage DOIT être ajouté, comme spécifié dans la [RFC4303], de telle sorte que les données à chiffrer (qui incluent les champs Longueur de bourrage ESP et Prochain en-tête) soient un multiple de 16 octets.

À cause de l'exigence de bourrage spécifique de l'algorithme, aucun bourrage supplémentaire n'est requis pour s'assurer que le texte chiffré se termine sur une limite de 4 octets. C'est-à-dire que maintenir une taille de bloc de 16 octets garantit que les champs Longueur de bourrage ESP et Prochain en-tête seront alignés à droite dans un mot de 4 octets). Un bourrage supplémentaire PEUT être inclus, comme spécifié dans la [RFC4303], pour autant que la taille de bloc de 16 octets soit conservée.

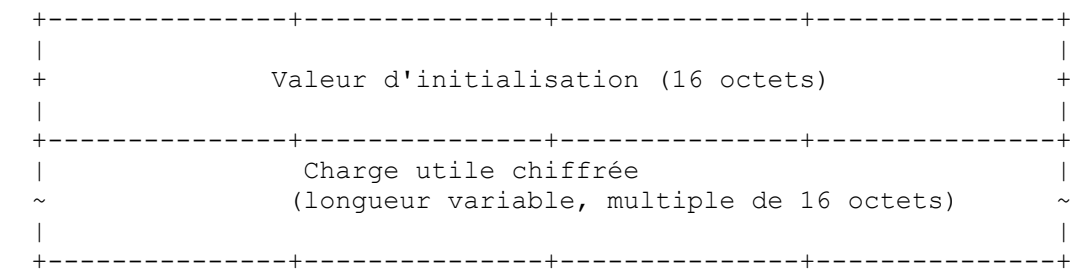
2.5 Performances

Les chiffres de performances de Camellia sont disponibles à [Camellia-Web]. Ce site de la Toile inclut aussi des

comparaisons de performances avec le chiffrement AES et les autres finalistes du concours AES. Le projet NESSIE [NESSIE] a rapporté les performances des mises en œuvre optimisées de façon indépendante.

3. Charge utile ESP

La charge utile ESP est constituée de l'IV suivie par un texte chiffré brut. Donc, le champ Charge utile, comme défini dans la [RFC4303], est coupé selon le diagramme suivant :



Le champ IV DOIT être de la même taille que la taille de bloc de l'algorithme de chiffrement utilisé. La IV DOIT être choisie au hasard, et DOIT être imprévisible.

Inclure la IV dans chaque datagramme assure que chaque datagramme reçu peut être déchiffré, même quand certains datagrammes sont abandonnés ou réordonnés dans le transit.

Pour éviter le chiffrement CBC de blocs de texte source très similaires dans des paquets différents, les mises en œuvre NE DOIVENT PAS utiliser un compteur ou autre source à faible distance de Hamming pour les IV.

3.1 Interactions algorithmiques ESP

Il n'y a actuellement pas de problème connu concernant les interactions entre Camellia et les autres aspects de ESP, comme l'utilisation de certains schémas d'authentification.

3.2 Matériel de chiffrement

Le nombre minimum de bits envoyés du protocole d'échange de clé à l'algorithme ESP doit être supérieur ou égal à la taille de clé. La clé de chiffrement et de déchiffrement du chiffrement est tirée des premiers 128, 192, ou 256 bits du matériel de chiffrement.

4. Interaction avec l'échange de clé Internet (IKE)

Camellia a été conçu pour suivre la même API que le chiffrement AES. Donc, cette section définit seulement l'identifiant de phase 1 et l'identifiant de phase 2. Toute autre considération relative à l'interaction avec IKE est identique à celle du chiffrement AES. On trouvera les détails dans la [RFC3602].

4.1 Identifiant de phase 1

Pour les négociations de phase 1, l'IANA a alloué l'identifiant d'algorithme de chiffrement 8 pour CAMELLIA-CBC.

4.2 Identifiant de phase 2

Pour les négociations de phase 2, l'IANA a alloué l'identifiant de transformation ESP 22 pour ESP_CAMELLIA.

5. Considérations sur la sécurité

Les mises en œuvre sont invitées à utiliser les plus grandes tailles de clé qu'elles peuvent, en tenant compte des considérations de performances pour leur matériel particulier et leur configuration de logiciel. Noter que le chiffrement affecte nécessairement les deux côtés d'un canal sécurisé, de sorte qu'il faut prendre en considération non seulement le côté client, mais aussi le côté serveur. Cependant, une taille de clé de 128 bits est considérée comme sûre pour l'avenir prévisible.

Aucun problème de sécurité n'a été trouvé dans Camellia [CRYPTREC], [NESSIE].

6. Considérations relatives à l'IANA

L'IANA a alloué l'identifiant d'algorithme de chiffrement 8 à CAMELLIA-CBC.

L'IANA a alloué l'identifiant de transformation ESP 22 à ESP_CAMELLIA.

7. Remerciements

Des portions de ce texte sont empruntées à la [RFC3602]. Ce travail a été fait quand le premier auteur travaillait pour NTT.

8. Références

8.1 Références normatives

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

[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.)*

8.2 Références pour information

[AES] NIST, FIPS PUB 197, "Advanced Encryption Standard (AES)," novembre 2001. http://csrc.nist.gov/publications/fips/fips197fips-197 .{ps,pdf}.

[Camellia-Web] Page d'accueil de Camellia : http://info.isl.ntt.co.jp/camellia/ .

[CRYPTO-S] Schneier, B., "Applied Cryptography Second Edition", John Wiley & Sons, New York, NY, 1995, ISBN 0-471-12845-7.

[CRYPTREC] Information-technology Promotion Agency (IPA), Japan, CRYPTREC. 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.ac.be/nessie/ .

[RFC2401] S. Kent et R. Atkinson, "Architecture de sécurité pour le protocole Internet", novembre 1998. (*Obsolète, voir* RFC4301)

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

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

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

[RFC3657] S. Moriai, A. Kato, "Utilisation de l'algorithme de chiffrement Camellia dans la syntaxe de message cryptographique (CMS)", janvier 2004. *(P.S.)*

[SP800-38a] Dworkin, M., "Recommendation for Block Cipher Modes of Operation - Methods and Techniques", NIST Special Publication 800-38A, décembre 2001.

Adresse des auteurs

Akihiro Kato
NTT Software Corporation
téléphone : +81-45-212-7934
Fax : +81-45-212-7410
mél : akato@po.ntts.co.jp

Shiho Moriai
Sony Computer Entertainment Inc.
téléphone : +81-3-6438-7523
Fax : +81-3-6438-8629
mél : camellia@isl.ntt.co.jp (Camellia)
shiho@rd.scei.sony.co.jp (Shiho Moriai)

Masayuki Kanda
NTT Corporation
téléphone : +81-46-859-2437
Fax : +81-46-859-3365
mél : kanda@isl.ntt.co.jp

Déclaration de droits de reproduction

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