Groupe de travail Réseau
Request for Comments : 5288
Catégorie : Sur la voie de la normalisation
Traduction Claude Brière de L'Isle

J. Salowey, Cisco Systems, Inc.
A. Choudhury, Cisco Systems, Inc.
D. McGrew, Cisco Systems, Inc.
août 2008

Suites de chiffrement AES en mode compteur Galois (GCM) pour TLS

Résumé
Le présent mémoire décrit l'utilisation de la norme de chiffrement évoluée (AES, *Advanced Encryption Standard*) en mode Galois/compteur (CGM, *Galois/Counter Mode*) comme opération authentifiée de sécurité de la couche transport (TLS, *Transport Layer Security*). GCM assure la confidentialité et l'authentification de l'origine des données, et peut être efficacement mis en œuvre dans du matériel à des vitesses de 10 gigabits par seconde et au-delà, et convient bien aussi pour les mises en œuvre de logiciel. Le présent mémoire définit des suites de chiffrement TLS qui utilisent AES-GCM avec RSA, DSA, et les mécanismes d'échange de clés fondés sur Diffie-Hellman.

Table des matières

1. Introduction

Le présent document décrit l'utilisation de AES [AES] en mode Galois/compteur [GCM] (AES-GCM) avec divers mécanismes d'échange de clés dans une suite de chiffrement pour TLS. AES-GCM est un chiffrement authentifié avec des données associées (AEAD, *Authenticated Encryption with Associated Data*) (comme défini dans TLS 1.2 [RFC5246]) qui fournit la confidentialité et l'authentification de l'origine des données. Les sections suivantes définissent les suites de chiffrement fondées sur RSA, DSA, et les échanges de clé Diffie-Hellman ; les suites de chiffrement fondées sur la cryptographie à courbe elliptique (ECC, *Elliptic Curve Cryptography*) sont définies dans un document distinct [RFC5289].

AES-GCM est non seulement efficace et sûr, mais les mises en œuvre matérielles peuvent réaliser de grandes vitesses avec un coût et une latence faibles, parce que le mode peut être traité en parallèle. Les applications qui exigent un haut débit de données peuvent bénéficier de ces mises en œuvre à grande vitesse. AES-GCM a été spécifié comme un mode qui peut être utilisé avec IPsec ESP [RFC4106] et la sécurité du contrôle de l'accès au support (MAC, *Media Access Control*) 802.1AE [IEEE8021AE].

2. Conventions utilisées dans ce document

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].

3. Suites de chiffrement AES-GCM

Les suites de chiffrement suivantes utilisent les nouveaux modes de chiffrement authentifié définis dans TLS 1.2 avec AES en mode Galois/compteur (GCM) [GCM] :

Suite de chiffrement TLS_RSA_WITH_AES_128_GCM_SHA256 = {0x00,0x9C}
Suite de chiffrement TLS_RSA_WITH_AES_256_GCM_SHA384 = {0x00,0x9D}
Suite de chiffrement TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 = {0x00,0x9E}
Suite de chiffrement TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 = {0x00,0x9F}
Suite de chiffrement TLS_DH_RSA_WITH_AES_128_GCM_SHA256 = {0x00,0xA0}
Suite de chiffrement TLS_DH_RSA_WITH_AES_256_GCM_SHA384 = {0x00,0xA1}
Suite de chiffrement TLS_DHE_DSS_WITH_AES_128_GCM_SHA256 = {0x00,0xA2}
Suite de chiffrement TLS_DHE_DSS_WITH_AES_256_GCM_SHA384 = {0x00,0xA3}
Suite de chiffrement TLS_DH_DSS_WITH_AES_128_GCM_SHA256 = {0x00,0xA4}
Suite de chiffrement TLS_DH_DSS_WITH_AES_256_GCM_SHA384 = {0x00,0xA5}
Suite de chiffrement TLS_DH_anon_WITH_AES_128_GCM_SHA256 = {0x00,0xA6}
Suite de chiffrement TLS_DH_anon_WITH_AES_256_GCM_SHA384 = {0x00,0xA7}

Ces suites de chiffrement utilisent les algorithmes de chiffrement authentifié AES-GCM avec données associées (AEAD) AEAD_AES_128_GCM et AEAD_AES_256_GCM décrits dans la [RFC5116]. Noter que chacun de ces algorithmes AEAD utilise une étiquette d'authentification de 128 bits avec GCM (en particulier, comme décrit au paragraphe 3.5 de la [RFC4366], l'extension "hmac tronqué" n'a pas d'effet sur les suites de chiffrement qui n'utilisent pas HMAC). Le "nom occasionnel" DEVRA être de 12 octets consistant en deux parties comme suit : (c'est un exemple de nom occasionnel "partiellement explicite" ; voir le paragraphe 3.2.1 de la [RFC5116]).

```
struct {
  sel opaque [4];
  nom_occasionnel_explicite opaque [8];
} GCMNonce;
```

Le sel est la partie "implicite" du nom occasionnel et n'est pas envoyé dans le paquet. Le sel est plutôt généré au titre du processus de prise de contact : il est soit le client_write_IV *(valeur d'initialisation écrite par le client)* (quand le client envoie) soit le server_write_IV *(valeur d'initialisation écrite par le serveur)* (quand le serveur envoie). La longueur du sel (SecurityParameters.fixed_iv_length) est de 4 octets.

Le nom_occasionnel_explicite est la partie "explicite" du nom occasionnel. Il est choisi par l'envoyeur et est porté dans chaque enregistrement TLS dans le champ GenericAEADCipher.nonce_explicit. La longueur du nom_occasionnel_explicite (SecurityParameters.record_iv_length) est de 8 octets.

Chaque valeur de nom_occasionnel_explicite DOIT être distincte pour chaque invocation distincte de la fonction de chiffrement GCM pour toute clé fixée. Manquer à satisfaire cette exigence d'unicité peut significativement dégrader la sécurité. Le nom_occasionnel_explicite PEUT être le numéro de séquence de 64 bits.

Les échanges de clé RSA, DHE_RSA, DH_RSA, DHE_DSS, DH_DSS, et DH_anon sont effectués comme défini dans la [RFC5246].

Les algorithmes de fonction pseudo-aléatoire (PRF, *Pseudo Random Function*) DEVRONT être comme suit :

Pour les suites de chiffrement qui se terminent avec _SHA256, la PRF est la PRF TLS [RFC5246] avec SHA-256 comme fonction de hachage.

Pour les suites de chiffrement qui se terminent avec _SHA384, la PRF est la PRF TLS [RFC5246] avec SHA-384 comme

fonction de hachage.

Les mises en œuvre DOIVENT envoyer l'alerte TLS "mauvais_enregistrement_de_mac" pour tous les types de défaillances rencontrés dans le traitement de l'algorithme AES-GCM.

4. Versions de TLS

Ces suites de chiffrement utilisent le chiffrement authentifié avec données supplémentaires défini dans TLS 1.2 [RFC5246]. Elles NE DOIVENT PAS être négociées dans les plus anciennes versions de TLS. Les clients NE DOIVENT PAS offrir ces suites de chiffrement si ils n'offrent pas TLS 1.2 ou plus récent. Les serveurs qui choisissent une version antérieure de TLS NE DOIVENT PAS choisir une de ces suites de chiffrement. Parce que TLS n'a pas de moyen pour que le client indique qu'il prend en charge TLS 1.2 mais pas de version antérieure, un serveur non conforme pourrait éventuellement négocier TLS 1.1 ou antérieur et choisir une des suites de chiffrement du présent document. Les clients DOIVENT vérifier la version TLS et générer une alerte fatale "paramètre_illégal" si ils détectent une version incorrecte.

5. Considérations relatives à l'IANA

L'IANA a alloué les valeurs suivantes aux suites de chiffrement définies dans le présent document :
Suite de chiffrement TLS_RSA_WITH_AES_128_GCM_SHA256 = {0x00,0x9C}
Suite de chiffrement TLS_RSA_WITH_AES_256_GCM_SHA384 = {0x00,0x9D}
Suite de chiffrement TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 = {0x00,0x9E}
Suite de chiffrement TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 = {0x00,0x9F}
Suite de chiffrement TLS_DH_RSA_WITH_AES_128_GCM_SHA256 = {0x00,0xA0}
Suite de chiffrement TLS_DH_RSA_WITH_AES_256_GCM_SHA384 = {0x00,0xA1}
Suite de chiffrement TLS_DHE_DSS_WITH_AES_128_GCM_SHA256 = {0x00,0xA2}
Suite de chiffrement TLS_DHE_DSS_WITH_AES_256_GCM_SHA384 = {0x00,0xA3}
Suite de chiffrement TLS_DH_DSS_WITH_AES_128_GCM_SHA256 = {0x00,0xA4}
Suite de chiffrement TLS_DH_DSS_WITH_AES_256_GCM_SHA384 = {0x00,0xA5}
Suite de chiffrement TLS_DH_anon_WITH_AES_128_GCM_SHA256 = {0x00,0xA6}
Suite de chiffrement TLS_DH_anon_WITH_AES_256_GCM_SHA384 = {0x00,0xA7}

6. Considérations sur la sécurité

Les considérations sur la sécurité de la [RFC5246] s'appliquent aussi au présent document. Le reste de cette section décrit les considérations sur la sécurité spécifiques des suites de chiffrement décrites dans ce document.

6.1 Réutilisation de compteur

La sécurité de AES-GCM exige que le compteur ne soit jamais réutilisé. La construction de valeur d'initialisation (IV) de la Section 3 est conçue pour empêcher la réutilisation du compteur.

Les mises en œuvre devraient aussi comprendre les considérations pratiques du traitement de l'IV mentionnées à la Section 9 de [GCM].

6.2 Recommandations pour les processeurs de chiffrements multiples

Si l'envoyeur utilise plusieurs processeurs de chiffrement, il DOIT s'assurer que, pour une clé particulière, chaque valeur du nom_occasionnel_explicite utilisée avec cette clé est distincte. Dans ce cas, chaque processeur de chiffrement DEVRAIT inclure, dans le nom_occasionnel_explicite, une valeur fixée distincte pour chaque processeur. Le format recommandé est

nom_occasionnel_explicite = FixeDistinct || Variable

où le champ FixeDistinct est distinct pour chaque processeur de chiffrement, mais est fixe pour un processeur donné, et le

champ Variable est distinct pour chaque nom occasionnel distinct utilisé par un processeur de chiffrement particulier. Quand cette méthode est utilisée, les champs FixeDistinct utilisés par les différents processeurs DOIVENT avoir la même longueur.

Dans les termes de la Figure 2 de la [RFC5116], le sel est la partie Fixe-Commune du nom occasionnel (il est fixé, et est commun à tous les processeurs de chiffrement) le champ FixeDistinct correspond exactement au champ Fixe-Distinct, le champ Variable correspond au champ Compteur, et la partie explicite correspond exactement au nom_occasionnel_explicite.

Pour être clair, on donne un exemple pour TLS dans lequel il y a deux processeurs de chiffrement distincts, dont chacun utilise un champ FixeDistinct de un octet :

Sel = eedc68dc
FixeDistinct = 01 (pour le premier processeur de chiffrement)
FixeDistinct = 02 (pour le second processeur de chiffrement)

Les noms occasionnels GCM générés par le premier processeur de chiffrement, et leur nom_occasionnel_explicite correspondant, sont :

Nom occasionnel GCM	nom_occasionnel_explicite
eedc68dc0100000000000000	0100000000000000
eedc68dc0100000000000001	0100000000000001
eedc68dc0100000000000002	0100000000000002

...

Les noms occasionnels GCM générés par le second processeur de chiffrement, et leur nom_occasionnel_explicite correspondant, sont :

Nom occasionnel GCM	nom_occasionnel_explicite
eedc68dc0200000000000000	0200000000000000
eedc68dc0200000000000001	0200000000000001
eedc68dc0200000000000002	0200000000000002

...

7. Remerciements

Le présent document emprunte beaucoup à la [RFC5289]. Les auteurs tiennent à remercier Alex Lam, Simon Josefsson, et Pasi Eronen qui ont fournit d'utiles commentaires durant la relecture de ce document.

8. Références

8.1 Références normatives

[AES] National Institute of Standards and Technology, "Advanced Encryption Standard (AES)", FIPS 197, novembre 2001.

[GCM] Dworkin, M., "Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC", National Institute of Standards and Technology SP 800-38D, novembre 2007.

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

[RFC5116] D. McGrew, "Interface et algorithmes pour le chiffrement authentifié", janvier 2008. *(P.S.)*

[RFC5246] T. Dierks, E. Rescorla, "Version 1.2 du protocole de sécurité de la couche Transport (TLS)", DOI 10.17487/RFC5246, août 2008. *(P.S.* ; *remplace* RFC3268, 4346, 4366 ; *MàJ* RFC4492 ; *rendue obsolète par la* RFC8446)

8.2 Références pour information

[IEEE8021AE] Institute of Electrical and Electronics Engineers, "Media Access Control Security", IEEE Standard 802.1AE, août 2006.

[RFC4106] J. Viega, D. McGrew, "Utilisation du mode Galois/Compteur (GCM) dans une encapsulation IPsec de charge utile de sécurité (ESP)", juin 2005. *(P.S.)*

[RFC4366] S. Blake-Wilson et autres, "Extensions de sécurité de la couche Transport (TLS)", avril 2006. (*Obsolète,* RFC5246) *(P.S.)*

[RFC5289] E. Rescorla, "Suites de chiffrement à courbe elliptique pour TLS avec SHA-256/384 et AES avec mode de compteur de Galois (GCM)", août 2008. *(Information)*

Adresse des auteurs

Joseph Salowey
Cisco Systems, Inc.
2901 3rd. Ave
Seattle, WA 98121
USA
mél : jsalowey@cisco.com

Abhijit Choudhury
Cisco Systems, Inc.
3625 Cisco Way
San Jose, CA 95134
USA
mél : abhijitc@cisco.com

David McGrew
Cisco Systems, Inc.
170 W Tasman Drive
San Jose, CA 95134
USA
mél : mcgrew@cisco.com

Déclaration complète de droits de reproduction

Remerciement
Le financement de la fonction d'édition des RFC est fourni par l'activité de soutien administratif de l'IETF (IASA).