Équipe d'ingénierie de l'Internet (IETF)
Request for Comments: 5669
Catégorie : Sur la voie de la normalisation
ISSN: 2070-1721

Traduction Claude Brière de L'Isle

S. Yoon, Korea Internet & Security Agency
J. Kim, Korea Internet & Security Agency
H. Park, Korea Internet & Security Agency
H. Jeong, Korea Internet & Security Agency
Y. Won, Korea Internet & Security Agency

août 2010

Algorithme de chiffrement SEED et utilisation avec le protocole de transport sûr en temps réel (SRTP)

Résumé
Le présent document décrit l'utilisation de l'algorithme de chiffrement de bloc SEED dans le protocole de transport sûr en temps réel (SRTP, *Secure Real-time Transport Protocol*) pour fournir la confidentialité au trafic du protocole de transport en temps réel (RTP, *Real-time Transport Protocol*) et pour le trafic de contrôle pour RTP, le protocole de contrôle du transport en temps réel (RTCP, *Real-time Transport Control Protocol*).

Statut de ce mémoire
Ceci est un document de l'Internet sur la voie de la normalisation.

Le présent document a été produit par l'équipe d'ingénierie de l'Internet (IETF). Il représente le consensus de la communauté de l'IETF. Il a subi une révision publique et sa publication a été approuvée par le groupe de pilotage de l'ingénierie de l'Internet (IESG). Tous les documents approuvés par l'IESG ne sont pas candidats à devenir une norme de l'Internet ; voir la Section 2 de la RFC5741.

Les informations sur le statut actuel du présent document, tout errata, et comment fournir des réactions sur lui peuvent être obtenues à http://www.rfc-editor.org/info/rfc5669

Table des matières

1. Introduction

Le présent document décrit l'utilisation de l'algorithme de chiffrement de bloc SEED [RFC4269] dans le protocole de transport sûr en temps réel (SRTP, *Secure Real-time Transport Protocol*) [RFC3711] pour fournir la confidentialité au trafic du protocole de transport en temps réel (RTP, *Real-time Transport Protocol*) [RFC3550] et pour le trafic de contrôle pour le protocole de contrôle du transport en temps réel (RTCP, *Real-time Transport Control Protocol*) [RFC3550].

1.1 SEED

SEED est un algorithme de chiffrement symétrique qui a été développé par l'agence coréenne de sécurité de l'information (KISA, *Korea Information Security Agency*) et un groupe d'experts, en 1998. La taille de bloc d'entrée/sortie de SEED est de 128 bits et la longueur de clé est aussi de 128 bits. SEED a une structure de Feistel à 16 tours. Une entrée de 128 bits est divisée en deux blocs de 64 bits et le bloc de 64 bits de droite est une entrée à la fonction de tours avec une sous clé de 64 bits générée à partir du programme de clés.

SEED est facilement mis en œuvre dans divers logiciels et matériels parce que il est conçu pour augmenter l'efficacité de la mémorisation et la simplicité de génération de clés sans dégrader la sécurité de l'algorithme. En particulier, il peut être effectivement adopté dans un environnent de calcul qui a des ressources restreintes comme les appareils mobiles, les cartes à mémoire, et autres.

SEED est une norme d'association industrielle nationale [TTASSEED] et est largement utilisé en Corée du Sud pour le commerce électronique et les services financiers sur PKI filaire et sans fil.

La spécification de l'algorithme et les identifiants d'objet sont décrits dans la [RFC4269]. La page d'accueil SEED, http://seed.kisa.ou.kr/eng/main.jsp, contient de nombreuses informations sur SEED, incluant des spécifications détaillées, un rapport d'évaluation, des vecteurs d'essai, et autres.

1.2 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].

1.3 Définitions

|| : enchaînement
XOU : ou exclusif

2. Transformations cryptographiques

Tous les algorithmes de chiffrement de bloc symétrique partagent des caractéristiques communes, incluant le mode, la taille de clé, les clés faibles, et la taille de bloc. Les paragraphes qui suivent contiennent la description des caractéristiques pertinentes de SEED.

SEED n'a pas de restrictions pour les modes de fonctionnement qui sont utilisés avec ce chiffrement de bloc. On définit trois modes de fonctionnement de SEED : (1) SEED en mode compteur, (2) SEED en mode compteur avec CBC-MAC (CCM) et (3) SEED en mode Galois/compteur (GCM).

2.1 Compteur

Le paragraphe 4.1.1 de la [RFC3711] définit le chiffrement AES en mode compteur, que le présent document appelle AES-CM. SEED en mode compteur est défini de manière similaire et est noté SEED-CTR. Les entrées de texte en clair au chiffrement de bloc sont formés comme dans AES-CM, et le résultat du chiffrement de bloc est traité comme dans AES-CM. La seule différence dans le traitement est que SEED-CTR utilise SEED comme primitive de chiffrement sous-jacente. Quand SEED-CTR est utilisé, il DOIT être utilisé seulement en conjonction avec une fonction d'authentification.

2.1.1 Authentification/intégrité de message : HMAC-SHA1

HMAC-SHA1 [RFC2104], comme défini au paragraphe 4.2.1 de la [RFC3711], DEVRA être le code d'authentification de message par défaut à utiliser avec SEED-CTR. La longueur de clé d'authentification de session par défaut DEVRA être de 160 bits, la longueur d'étiquette d'authentification par défaut DEVRA être 80 bits, et SRTP_PREFIX_LENGTH *(longueur de préfixe SRTP)* DEVRA être zéro pour HMAC-SHA1. Pour SRTP, de plus petites valeurs sont NON RECOMMANDÉES mais PEUVENT être utilisées après considération attentive des problèmes discutés dans les paragraphes 7.5 et 9.5 de la [RFC3711].

2.2 Compteur avec CBC-MAC (CCM)

CCM [RFC3610] est le mode générique de chiffrement de bloc d'authentification et de chiffrement. Dans cette spécification, CCM utilisé avec le chiffrement de bloc SEED est noté SEED-CCM.

Le paragraphe 3.3 de la [RFC3711] définit les procédures pour construire ou authentifier et déchiffrer les paquets SRTP. Pour SEED-CCM, cependant, l'envoyeur effectue l'étape 7 avant l'étape 5 et le receveur effectue la seconde moitié de l'étape 5 (vérification) après l'étape 6. Cela signifie que l'authentification est effectuée sur le texte en clair plutôt que sur le texte chiffré. Cela s'applique également au protocole de contrôle de transport sûr en temps réel (SRTCP, *Secure Real-time Transport Control Protocol)*.

Tous les paquets SRTP DOIVENT être authentifiés et chiffrés. À la différence de SRTP, le chiffrement du paquet SRTCP est facultatif (mais l'authentification est obligatoire). Un envoyeur peut choisir quels paquets chiffrer et il indique ce choix avec un fanion de chiffrement de 1 bit (situé dans le bit de gauche du mot de 32 bits que contient l'indice SRTCP).

SEED-CCM a deux paramètres :

M : M indique la taille de l'étiquette d'authentification. Dans SRTP, une étiquette complète d'authentification de 80 bits DEVRAIT être utilisée et une mise en œuvre de cette spécification DOIT prendre en charge M valeurs de 10 octets.

L : L indique la taille du champ Longueur en octets. Le nombre d'octets dans le nom occasionnel DOIT être 12, c'est-à-dire, L est 3.

SEED-CCM a quatre entrées :

Clé : une seule clé est utilisée pour calculer l'étiquette d'authentification (en utilisant CBC-MAC) et pour effectuer le chiffrement de charge utile en utilisant le mode compteur. SEED prend seulement en charge une taille de clé de 128 bits.

Nom occasionnel : La taille du nom occasionnel dépend de la valeur choisie pour le paramètre L. Elle est de 15 - L octets. L égale 3, et donc la taille du nom occasionnel égale 12 octets.

Texte en clair : dans le cas de SRTP, la charge utile du paquet RTP, le bourrage RTP, et le champ Compte de bourrage RTP (si les deux derniers champs sont présents) sont traités comme du texte en clair. Dans le cas de SRTCP, quand le fanion de chiffrement est établi à 1, la portion chiffrée décrite dans la Figure 2 de la [RFC3711] est traitée comme du texte en clair. Quand le fanion de chiffrement est réglé à 0, la longueur du texte en clair est zéro.

Données d'authentification supplémentaires (AAD, *Additional Authentication Data*) : dans le cas de SRTP, l'en-tête du paquet RTP, incluant l'identifiant de la source contributive (CSRC, *contributing source*) (si présent) et l'extension d'en-tête RTP (si présente) est considéré comme AAD. Dans le cas de SRTCP, quand le fanion Chiffrement est réglé à 0, la portion d'authentification décrite dans la Figure 2 de la [RFC3711] est traitée comme AAD. Quand le fanion de chiffrement est établi à 1, les 8 premiers octets, le fanion de chiffrement, et l'indice SRTCP sont traités comme AAD.

SEED-CCM accepte ces quatre entrées et retourne un champ de texte chiffré.

2.3 Mode Galois/compteur (GCM)

GCM est un mode de chiffrement de bloc qui fournit à la fois la confidentialité et l'authentification de l'origine des données [GCM]. GCM utilisé avec le chiffrement de bloc SEED est noté SEED-GCM.

SEED-GCM a quatre entrées : une clé, un texte en clair, un nom occasionnel, et les données authentifiées supplémentaires (AAD, *additional authenticated data*) toutes décrites au paragraphe 2.2.

La longueur de l'étiquette, notée t, en bits est 12, et une étiquette d'authentification d'une longueur de 12 octets (96 bits) est utilisée.

3. Format de nom occasionnel pour CCM et GCM

3.1 Nom occasionnel pour SRTP

Le nom occasionnel pour SRTP DEVRA être formé de la façon suivante :

Nom occasionnel = (16 bits of zéros || SSRC || ROC || SEQ) OUX Sel

Le SSRC de 4 octets et le SEQ de 2 octets DEVRONT être pris de l'en-tête RTP. Le ROC de 4 octets est pris du contexte cryptographique. Le sel de 12 octets DEVRA être produit par la fonction de déduction de clé de SRTP.

3.2 Nom occasionnel pour SRTCP

Le nom occasionnel *(nonce)* pour SRTCP DEVRA être formé de la façon suivante :

Nom occasionnel = (16 bits of zéros || SSRC || 16 bits of zéros || Indice SRTCP) OUX Sel

Le SSRC de 4 octets DEVRA être pris de l'en-tête RTCP et l'indice SRTCP de 31 bits (mis en paquets remplis de zéros et justifié à droite dans un champ de 4 octets) est en provenance de chaque paquet. Le sel de 12 octets DEVRA être produit par la fonction de déduction de clé de SRTP.

4. Déduction de clé : PRF SEED-CTR

Le paragraphe 4.3.3 de la [RFC3711] définit la fonction de déduction de clé AES-128 en mode compteur, qui est aussi appelée "PRF AES-CM". La PRF SEED-CTR est définie d'une manière similaire, mais avec chaque invocation de AES remplacée par une invocation de SEED.

La PRF actuellement définie, chiffrée par la clé maîtresse de 128 bits, a une taille de bloc d'entrée m = 128 et peut produire des résultats de n bits pour n jusqu'à 2^23. SEED-PRF_n(k_master, x) DEVRA être SEED en mode compteur, comme décrit au paragraphe 2.1 ; il DEVRA être appliqué à la clé k_master, avoir un IV égal à (x*2^16), et avoir le flux de clé de sortie tronqué aux n premiers bits (ceux de gauche).

5. Transformations de mise en œuvre obligatoire

"De mise en œuvre obligatoire" signifie conforme à la présente spécification, et que le Tableau 1 dans le présent document ne se substitue pas à un tableau similaire de la Section 5 de la [RFC3711]. Une mise en œuvre de RTP qui prend en charge SEED DOIT mettre en œuvre les modes mentionnées dans le Tableau 1 du présent document.

	De mise en œuvre obligatoire	**Facultatif**
Chiffrement	SEED-CTR	SEED-CCM, SEED-GCM
Intégrité de message	HMAC-SHA1	SEED-CCM, SEED-GCM
Déduction de clé (PRF)	SEED-CTR	-

Tableau 1 : Transformations de mise en œuvre obligatoire et facultatives dans SRTP et SRTCP

6. Considérations sur la sécurité

Aucun problème de sécurité n'a été trouvé sur SEED. SEED est sûr contre toutes les attaques connues, y compris la cryptanalyse différentielle, la cryptanalyse linéaire, et les attaques de clé en rapport. L'attaque la plus connue est seulement une recherche exhaustive sur la clé. Pour plus de considérations sur la sécurité, le lecteur est encouragé à lire [SEED-EVAL].

Voir la [RFC3610] et [GCM] pour les considérations sur la sécurité concernant respectivement les modes de fonctionnement CCM et GCM. Dans le contexte de SRTP, les procédures de la [RFC3711] assurent la propriété critique de non réutilisation des valeurs de compteur.

7. Considérations relatives à l'IANA

La [RFC4568] définit les "suites de chiffrement" SRTP. Afin de permettre au protocole de description de session (SDP, *Session Description Protocol*) de signaler l'utilisation des algorithmes définis dans le présent document, l'IANA a enregistré les suites de chiffrement suivantes dans le sous registre des suites de chiffrement SRTP sous les transports de flux de supports des descriptions de sécurité SDP :

SEED_CTR_128_HMAC_SHA1_80
SEED_128_CCM_80
SEED_128_GCM_96

8. Remerciements

Les auteurs tiennent à remercier David McGrew, Eric Rescorla, Alexey Melnikov, Alfred Hoenes, Colin Perkins, Young-Chan Shin, le groupe de travail AVT (en particulier, ses présidents Roni Even et Tom Taylor) et les directeurs de la zone Applications et infrastructure en temps réel pour leurs relectures et leur soutien.

9. Références

9.1 Références normatives

[GCM] Dworkin, M., "NIST Special Publication 800-38D: Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC", U.S. National Institute of Standards and Technology, http://csrc.nist.gov/publications/nistpubs/800-38D/SP-800-38D.pdf

[RFC2104] H. Krawczyk, M. Bellare et R. Canetti, "HMAC : Hachage de clés pour l'authentification de message", février 1997, DOI 10.17487/RFC2104.

[RFC2119] S. Bradner, "Mots clés à utiliser dans les RFC pour indiquer les niveaux d'exigence", BCP 14, mars 1997. DOI 10.17487/RFC2119, *(MàJ par* RFC8174)

[RFC3550] H. Schulzrinne, S. Casner, R. Frederick et V. Jacobson, "RTP : un protocole de transport pour les applications en temps réel", STD 64, DOI 10.17487/RFC3550, juillet 2003. *(MàJ par* RFC7164, RFC7160, RFC8083, RFC8108, RFC8860)

[RFC3610] D. Whiting, R. Housley, N. Ferguson, "Compteur avec CBC-MAC (CCM)", septembre 2003. *(Information)*

[RFC3711] M. Baugher et autres, "Protocole de transport sécurisé en temps réel (SRTP)", mars 2004, DOI 10.17487/RFC3711. *(P.S. ; MàJ par* RFC9335*)*

[RFC4269] H.J. Lee et autres, "Algorithme de chiffrement SEED", décembre 2005. *(Remplace* RFC4009*) (Information)*

[RFC4568] F. Andreasen et autres, "Définition d'attributs de sécurité dans le protocole de description de session (SDP) pour les flux de support", juillet 2006. *(P.S.)*

[TTASSEED] Telecommunications Technology Association (TTA), South Korea, "128-bit Symmetric Block Cipher (SEED)", TTAS.KO-12.0004/R1, décembre 2005, http://www.tta.or.kr/English/index.jsp.

9.2 Références pour information

[SEED-EVAL] KISA, "Self Evaluation Report", http://seed.kisa.or.kr/eng/main.jsp

Appendice A. Vecteurs d'essai

Toutes les valeurs sont en hexadécimal.

A.1 Vecteurs d'essai SEED-CTR

Clé de session : 0c5ffd37a11edc42c325287fc0604f2e
Compteur de retournement : 00000000
Numéro de séquence : 315e
SSRC : 20e8f5eb
Clé d'authentification : f93563311b354748c978913795530631
Sel de session : cd3a7c42c671e0067a2a2639b43a
Vecteur d'initialisation : cd3a7c42e69915ed7a2a263985640000

Charge utile RTP :
f57af5fd4ae19562976ec57a5a7ad55a5af5c5e5c5fdf5c55ad57a4a7272d57262e9729566ed66e97ac54a4a5a7ad5e15ae5fdd5f
d5ac5d56ae56ad5c572d54ae54ac55a956afd6aed5a4ac562957a9516991691d572fd14e97ae962ed7a9f4a955af572e162f57a
956666e17ae1f54a95f566d54a66e16e4afd6a9f7ae1c5c55ae5d56afde916c5e94a6ec56695e14afde1148416e94ad57ac5146e
d59d1cc5

Charge utile RTP chiffrée :
df5a89291e7e383e9beff765e691a73749c9e33139ad3001cd8da73ad07f69a2805a70358b5c7c8c60ed359f95cf5e08f713c53f
f7b808250d79a19ccb8d10734e3cb72ed1f0a4e85b002b248049ab0763dbe571bec52cf9153fdf2019e421ef779cd6f4bd1c821
1da8c272e2fce43934b9eabb87362510f254149f992599036f5e43102327db1ac5e78adc4f66546ed7abfb5a4db320fb7b9c52a
61bc554e44

Étiquette d'authentification : a5cdaa4d9edc53763855

A.2 Vecteurs d'essai SEED-CCM

Clé : 974bee725d44fc3992267b284c3c6750
Compteur de retournement : 00000000
Numéro de séquence : 315e
SSRC : 20e8f5eb

Nom occasionnel : 000020e8f5eb00000000315e

Charge utile :
f57af5fd4ae19562976ec57a5a7ad55a5af5c5e5c5fdf5c55ad57a4a7272d57262e9729566ed66e97ac54a4a5a7ad5e15ae5fdd5f
d5ac5d56ae56ad5c572d54ae54ac55a956afd6aed5a4ac562957a9516991691d572fd14e97ae962ed7a9f4a955af572e162f57a
956666e17ae1f54a95f566d54a66e16e4afd6a9f7ae1c5c55ae5d56afde916c5e94a6ec56695e14afde1148416e94ad57ac5146e
d59d1cc5

AAD : 8008315ebf2e6fe020e8f5eb

Charge utile RTP chiffrée :
486843a881df215a8574650ddabf5dbb2650f06f51252bccaeb4012899d6d71e30c64dad5ead5d8ba65ffe9d79aaf30dc9e6334
490c07e7533d704114a9006ecb3b3bff59ecf585485bc0bd286ed434cfd684d19a1ad514ca5f37b71d93288c07cf4d5e9b83db8
becc8c692a7279b6a9ac62ba970fc54f46dcc926d434c0b5ad8678fbf0e7a03037924dae342ef64fa65b8eaea260fecb477a57e3
919c5dab82

Étiquette d'authentification : b0a8274cf6a8bb6cc466

A.3 Vecteurs d'essai SEED-GCM

Clé : e91e5e75da65554a48181f3846349562
Compteur de retournement : 00000000
Numéro de séquence : 315e
SSRC : 20e8f5eb
Nom occasionnel : 000020e8f5eb00000000315e

Charge utile :
f57af5fd4ae19562976ec57a5a7ad55a5af5c5e5c5fdf5c55ad57a4a7272d57262e9729566ed66e97ac54a4a5a7ad5e15ae5fdd5f
d5ac5d56ae56ad5c572d54ae54ac55a956afd6aed5a4ac562957a9516991691d572fd14e97ae962ed7a9f4a955af572e162f57a
956666e17ae1f54a95f566d54a66e16e4afd6a9f7ae1c5c55ae5d56afde916c5e94a6ec56695e14afde1148416e94ad57ac5146e
d59d1cc5

AAD : 8008315ebf2e6fe020e8f5eb

Charge utile RTP chiffrée :
8a5363682c6b1bbf13c0b09cf747a5512543cb2f129b8bd0e92dfadf735cda8f88c4bbf90288f5e58d20c4f1bb0d58446ea0091
03ee57ba99cdeabaaa18d4a9a05ddb46e7e5290a5a2284fe50b1f6fe9ad3f1348c354181e85b24f1a552a1193cf0e13eed5ab95a
e854fb4f5b0edb2d3ee5eb238c8f4bfb136b2eb6cd78760420680ce1879100014f140a15e07e70133ed9cbb6d57b75d574acb0
087eefbac99

Étiquette d'authentification : 36cd9ae602be3ee2cd8d5d9d

Adresse des auteurs

Seokung Yoon
Korea Internet & Security Agency
IT Venture Tower, Jungdaero 135
Songpa-gu, Seoul, Korea 138-950
mél : seokung@kisa.or.kr

Joongman Kim
Korea Internet & Security Agency
IT Venture Tower, Jungdaero 135
Songpa-gu, Seoul, Korea 138-950
mél : seopo@kisa.or.kr

Haeryong Park
Korea Internet & Security Agency
IT Venture Tower, Jungdaero 135
Songpa-gu, Seoul, Korea 138-950
mél : hrpark@kisa.or.kr

Hyuncheol Jeong
Korea Internet & Security Agency
IT Venture Tower, Jungdaero 135
Songpa-gu, Seoul, Korea 138-950
mél : hcjung@kisa.or.kr

Yoojae Won
Korea Internet & Security Agency
IT Venture Tower, Jungdaero 135
Songpa-gu, Seoul, Korea 138-950
mél : yjwon@kisa.or.kr