Groupe de travail Réseau
Request for Comments : 4196
Catégorie : Sur la voie de la normalisation

H.J. Lee, KISA
J.H. Yoon, KISA
S.L. Lee, KISA
J.I. Lee, KISA

Traduction Claude Brière de L'Isle
octobre 2005

Algorithme de chiffrement SEED et son utilisation avec IPsec

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

Table des matières

1. Introduction

1.1 SEED

SEED est une norme nationale d'association industrielle [TTASSEED] qui est largement utilisée en Corée du Sud pour le commerce électronique et les services financiers qui sont effectués sur des communications filaires et sans fil.

SEED est un chiffrement de bloc à clés symétriques de128 bits qui a été développé par KISA (Korea Information Security Agency) et un groupe d'experts depuis 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 à16 tours. Une entrée de 128 bits est divisée en deux blocs de 64 bits,

et le bloc de 64 bits de droite est entré dans la fonction de répétition avec une sous clé de 64 bits qui est générée à partir du programme de génération de clés.

SEED est facilement mis en œuvre dans divers logiciels et matériels, et il peut être effectivement adapté à un environnement de calcul à ressources restreintes, comme des appareils mobiles et des cartes à mémoire.

SEED est robuste contre les attaques connues incluant la cryptanalyse différentielle (DC, *Differential cryptanalysis*), la cryptanalyse linéaire (LC, *Linear cryptanalysis*) et les attaques de clé qui s'y rapportent. SEED est passé par de larges procédures d'examen publiques. Il a été évalué et est considéré comme cryptographiquement sûr par des organisations crédibles comme le JTC 1/SC 27 ISO/CEI [ISOSEED] et les comités de recherche et d'évaluation cryptographique (CRYPTREC, *Cryptography Research and Evaluation Committees*) du Japon [CRYPTREC].

Le reste du présent document spécifie l'utilisation de SEED dans le contexte de IPsec ESP. Pour plus d'informations sur la façon dont les diverses pièces de ESP s'assemblent pour assurer des services de sécurité, se référer aux [RFC2401], [RFC2406], et [RFC2411].

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].

2. Algorithme de chiffrement SEED

Tous les algorithmes de chiffrement à bloc symétrique partagent des caractéristiques et des 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 SEED.

La spécification de l'algorithme et des identifiants d'objets est décrite dans [ISOSEED] et la [RFC4009]. La page d'accueil de SEED, http://www.kisa.or.kr/seed/seed_eng.html, contient de nombreuses informations sur SEED, incluant une spécification détaillée, un rapport d'évaluation, des vecteurs d'essai, etc..

2.1 Mode

Le NIST a défini cinq modes de fonctionnement pour la norme de chiffrement évolué (AES, *Advanced Encryption Standard*) [AES] et d'autre chiffrements approuvés par FIPS [MODES] : le chaînage de bloc de chiffrement (CBC, *Cipher Block Chaining*), le mode dictionnaire (ECB, *Electronic Codebook*), le mode rebouclage du chiffrement (CFB, *Cipher FeedBack*), le mode rebouclage de la sortie (OFB, *Output FeedBack*), et le mode compteur (CTR, *Counter*). Le mode CBC est bien défini et bien compris pour les chiffrements symétriques, et est actuellement exigé pour tous les autres chiffrements d'ESP. Le présent document spécifie l'utilisation du chiffrement SEED en mode CBC au sein de ESP. Ce mode exige une valeur d'initialisation (IV, *Initialization Vector*) qui a la même taille que le bloc. L'utilisation d'IV générées au hasard empêche la génération de texte chiffré identique à partir de paquets qui ont des données identiques qui s'étendent sur le premier bloc de la taille de bloc de l'algorithme de chiffrement.

La IV est OUixée avec le premier bloc de texte source avant qu'il soit chiffré. Pour les blocs qui suivent, le bloc de texte chiffré précédent est OUixé avec le texte source en cours avant qu'il soit chiffré.

Plus d'informations sur le mode CBC figurent dans [MODES] et [CRYPTO-S]. Pour l'utilisation du mode CBC dans ESP avec un chiffrement à 64 bits, voir la [RFC2451].

2.2 Taille de clés et nombre de tours

SEED prend en charge des clés de 128 bits et a la structure de Feistel à seize tours.

2.3 Clés faibles

Au moment de la rédaction du présent document, il n'y a pas de clés faibles connues pour SEED.

2.4 Taille de bloc et bourrage

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

Le bourrage est exigé par SEED pour conserver une taille de bloc de 16 octets (128 bits). Le bourrage DOIT être ajouté, comme spécifié dans la [RFC2406], afin que les données à chiffrer (qui incluent les champs Longueur de bourrage ESP et Prochain en-tête) aient une longueur qui soit un multiple de 16 octets.

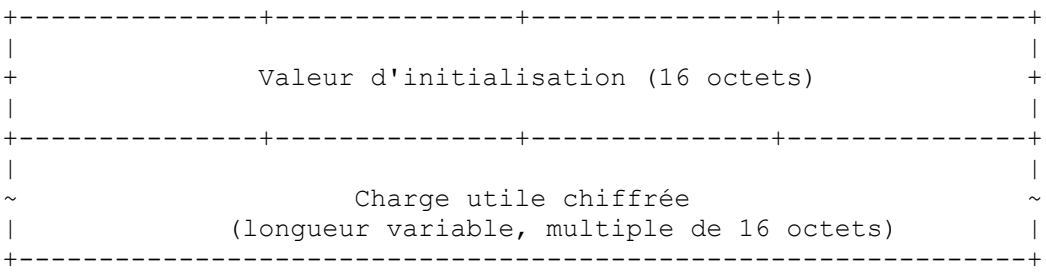
À cause de l'exigence de bourrage spécifique de l'algorithme, aucun bourrage supplémentaire n'est exigé pour assurer que le texte chiffré se termine sur une limite de 4 octets (c'est-à-dire, que conserver une taille de bloc de 16 octets garantit que les champs Longueur de bourrage ESP et Prochain en-tête seront bien alignés sur un mot de 4 octets). Un bourrage supplémentaire PEUT être inclus, comme spécifié dans la [RFC2406], pour autant que la taille de bloc de 16 octets soit conservée.

2.5 Performances

Les chiffres de performance de SEED sont disponibles à http://www.kisa.or.kr/seed/seed_eng.html

3. Charge utile ESP

La charge utile ESP est constituée de la valeur d'initialisation (IV) de 16 octets suivie par la charge utile chiffrée. Donc, le champ Charge utile, comme défini dans la [RFC2406], est divisé selon le diagramme suivant :



Le champ IV DOIT avoir la même taille que la taille de bloc de l'algorithme de chiffrement utilisé. La IV DOIT être choisie de façon aléatoire et DOIT être imprévisible.

Inclure l'IV dans chaque datagramme assure que le déchiffrement de chaque datagramme reçu peut être effectué, même quand certains datagrammes sont éliminés ou réarrangés 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.

4. Vecteurs d'essais

Les deux premiers essais vérifient le chiffrement SEED-CBC. Chaque cas d'essai inclut une clé, le texte source, et le texte chiffré résultant. Toutes les données sont des nombres hexadécimaux (sans préfixe "0x").

Les 4 derniers cas d'essai illustrent un échantillon de paquets ESP utilisant SEED-CBC comme chiffrement. Toutes les données sont des nombres hexadécimaux (sans préfixe "0x").

Cas n° 1 : Chiffrement de 32 octets (2 blocs) en utilisant SEED-CBC avec une clé de 128 bits
Clé : ed2401ad 22fa2559 91bafdb0 1fefd697
IV : 93eb149f 92c9905b ae5cd34d a06c3c8e
Texte source : b40d7003 d9b6904b 35622750 c91a2457 5bb9a632 364aa26e 3ac0cf3a 9c9d0dcb
Texte chiffré : f072c5b1 a0588c10 5af8301a dcd91dd0 67f68221 55304bf3 aad75ceb 44341c25

Cas n° 2 : Chiffrement de 64 octets (4 blocs) en utilisant SEED-CBC avec une clé de 128 bits
Clé : 88e34f8f 081779f1 e9f39437 0ad40589
IV : 268d66a7 35a81a81 6fbad9fa 36162501

Texte source : d76d0d18 327ec562 b15e6bc3 65ac0c0f 8d41e0bb 938568ae ebfd92ed 1affa096 394d20fc 5277ddfc
4de8b0fc e1eb2b93 d4ae40ef 4768c613 b50b8942 f7d4b9b3
Texte chiffré : a293eae9 d9aebfac 37ba714b d774e427 e8b706d7 e7d9a097 228639e0 b62b3b34 ced11609 cef2abaa
ec2edf97 9308f379 c31527a8 267783e5 cba35389 82b48d06

Cas n° 3 : Exemple de paquet ESP en mode transport (ping 192.168.123.100)
Clé : 90d382b4 10eeba7a d938c46c ec1a82bf
SPI : 4321
Adresse de source : 192.168.123.3
Adresse de destination : 192.168.123.100
Numéro de séquence : 1
IV : e96e8c08 ab465763 fd098d45 dd3ff893

Paquet d'origine :
En-tête IP (20 octets) : 45000054 08f20000 4001f9fe c0a87b03 c0a87b64
Données (64 octets) :
08000ebd a70a0000 8e9c083d b95b0700
08090a0b 0c0d0e0f 10111213 14151617
18191a1b 1c1d1e1f 20212223 24252627
28292a2b 2c2d2e2f 30313233 34353637

Données augmentées avec :
Bourrage : 01020304 05060708 090a0b0c 0d0e
Longueur de bourrage : 0e
Prochain en-tête : 01 (ICMP)

Données avant chiffrement avec bourrage, longueur de bourrage et prochain en-tête (80 octets) :
08000ebd a70a0000 8e9c083d b95b0700
08090a0b 0c0d0e0f 10111213 14151617
18191a1b 1c1d1e1f 20212223 24252627
28292a2b 2c2d2e2f 30313233 34353637
01020304 05060708 090a0b0c 0d0e0e01

Paquet après chiffrement avec SPI, numéro de séquence, IV :
En-tête IP : 45000054 08f20000 4001f9fe c0a87b03 c0a87b64
SPI/ n° de séquence : 00004321 00000001
IV : e96e8c08 ab465763 fd098d45 dd3ff893
Données chiffrées (80 octets) :
e7ebaa03 cf45ef09 021b3011 b40d3769
be96ebae cd4222f6 b6f84ce5 b2d5cdd1
60eb6b0e 5a47d16a 501a4d10 7b2d7cc8
ab86ba03 9a000972 66374fa8 f87ee0fb
ef3805db faa144a2 334a34db 0b0f81ca

Cas n° 4 : Exemple de paquet ESP en mode transport (ping -p 77 -s 20 192.168.123.100)
Clé : 90d382b4 10eeba7a d938c46c ec1a82bf
SPI : 4321
Adresse de source : 192.168.123.3
Adresse de destination : 192.168.123.100
Numéro de séquence : 8
IV : 69d08df7 d203329d b093fc49 24e5bd80

Paquet d'origine :
En-tête IP (20 octets) : 45000030 08fe0000 4001fa16 c0a87b03 c0a87b64
Données (28 octets) : 0800b5e8 a80a0500 a69c083d 0b660e00 77777777 77777777 77777777

Données augmentées de :
Bourrage : 0102
Longueur de bourrage : 02
Prochain en-tête : 01 (ICMP)

Données avant chiffrement avec bourrage, longueur de bourrage et prochain en-tête (32 octets) :
0800b5e8 a80a0500 a69c083d 0b660e00

77777777 77777777 77777777 01020201

Paquet après chiffrement avec SPI, numéro de séquence, IV :
En-tête IP : 4500004c 08fe0000 4032f9c9 c0a87b03 c0a87b64
SPI/n° séquence : 00004321 00000008
IV : 69d08df7 d203329d b093fc49 24e5bd80
Données chiffrées (32 octets) :
b9ad6e19 e9a6a2fa 02569160 2c0af541
db0b0807 e1f660c7 3ae2700b 5bb5efd1

Cas n° 5 : Exemple de paquet ESP en mode tunnel (ping 192.168.123.200)
Clé : 01234567 89abcdef 01234567 89abcdef
SPI : 8765
Adresse de source : 192.168.123.3
Adresse de destination : 192.168.123.200
Numéro de séquence : 2
IV : f4e76524 4f6407ad f13dc138 0f673f37

Paquet d'origine :
En-tête IP (20 octets) : 45000054 09040000 4001f988 c0a87b03 c0a87bc8
Données (64 octets) :
08009f76 a90a0100 b49c083d 02a20400
08090a0b 0c0d0e0f 10111213 14151617
18191a1b 1c1d1e1f 20212223 24252627
28292a2b 2c2d2e2f 30313233 34353637

Données augmentées avec :
Bourrage : 01020304 05060708 090a
Longueur de bourrage : 0a
Prochain en-tête : 04 (IP dans IP)

Données avant chiffrement avec bourrage, longueur de bourrage et prochain en-tête (96 octets) :
45000054 09040000 4001f988 c0a87b03
c0a87bc8 08009f76 a90a0100 b49c083d
02a20400 08090a0b 0c0d0e0f 10111213
14151617 18191a1b 1c1d1e1f 20212223
24252627 28292a2b 2c2d2e2f 30313233
34353637 01020304 05060708 090a0a04

Paquet après chiffrement avec SPI, numéro de séquence, IV :
En-tête IP : 4500008c 09050000 4032f91e c0a87b03 c0a87bc8
SPI/n° séquence : 00008765 00000002
IV : f4e76524 4f6407ad f13dc138 0f673f37
Données chiffrées (96 octets) :
2638aa7b 05e71b54 9348082b 67b47b26
c565aed4 737f0bcb 439c0f00 73e7913c
3c8a3e4f 5f7a5062 003b78ed 7ca54a08
c7ce047d 5bec14e4 8cba1005 32a12097
8d7f5503 204ef661 729b4ea1 ae6a9178
59a5caac 46e810bd 7875bd13 d6f57b3d

Cas n° 6 : Exemple de paquet ESP en mode tunnel (ping -p ff -s 40 192.168.123.200)
Clé : 01234567 89abcdef 01234567 89abcdef
SPI : 8765
Adresse de source : 192.168.123.3
Adresse de destination : 192.168.123.200
Numéro de séquence : 5
IV : 85d47224 b5f3dd5d 2101d4ea 8dffab22

Paquet d'origine :
En-tête IP (20 octets) : 45000044 090c0000 4001f990 c0a87b03 c0a87bc8
Données (48 octets) :
0800d63c aa0a0200 c69c083d a3de0300

ffffffff ffffffff ffffffff ffffffff
ffffffff ffffffff ffffffff ffffffff

Données augmentées avec :
Bourrage : 01020304 05060708 090a
Longueur de bourrage : 0a
Prochain en-tête : 04 (IP dans IP)

Données avant chiffrement avec bourrage, longueur de bourrage et prochain en-tête (80 octets) :
45000044 090c0000 4001f990 c0a87b03
c0a87bc8 0800d63c aa0a0200 c69c083d
a3de0300 ffffffff ffffffff ffffffff
ffffffff ffffffff ffffffff ffffffff
ffffffff 01020304 05060708 090a0a04

Paquet après chiffrement avec SPI, numéro de séquence, IV :
En-tête IP : 4500007c 090d0000 4032f926 c0a87b03 c0a87bc8
SPI/n° séquence : 00008765 00000005
IV : 85d47224 b5f3dd5d 2101d4ea 8dffab22
Données chiffrées (80 octets) :
311168e0 bc36ac4e 59802bd5 192c5734
8f3d29c8 90bab276 e9db4702 91f79ac7
79571929 c170f902 ffb2f08b d448f782
31671414 ff29b7e0 168e1c87 09ba2b67
a56e0fbc 4ff6a936 d859ed57 6c16ef1b

5. Interaction avec IKE

Cette section décrit l'utilisation de IKE [RFC2409] pour établir des associations de sécurité (SA) ESP IPsec qui emploient SEED en mode CBC.

5.1 Identifiant de phase 1

Pour les négociations de phase 1, l'identifiant d'objet de SEED-CBC est défini dans la [RFC4009].

IDENTIFIANT D'OBJET algorithme ::= { iso(1) member-body(2) korea(410) kisa(200004) algorithm(1) }

IDENTIFIANT D'OBJET id-seedCBC ::= { algorithme seedCBC(4) }

5.2 Identifiant de phase 2

Pour les négociations de phase 2, l'IANA a alloué un identifiant de transformation ESP de (21) pour ESP_SEED_CBC.

5.3 Attribut Longueur de clé

Comme SEED prend en charge des longueurs de clé de 128 bits, l'attribut Longueur de clé est réglé à 128 bits.

5.4 Considérations d'algorithme de hachage

HMAC-SHA-1 [RFC2404] et HMAC-MD5 [RFC2403] sont actuellement considérés comme de force suffisante pour servir à la fois de générateurs IKE de clés SEED de 128 bits et comme authentifiants ESP pour le chiffrement SEED utilisant des clés de 128 bits.

6. Considérations sur la sécurité

Aucun problème de sécurité n'a été trouvé dans SEED. SEED est sûr contre toutes les attaques connues, y compris de cryptanalyse différentielle, cryptanalyse linéaire, et les attaques de clés en rapport. L'attaque la mieux connue est seulement

une recherche exhaustive sur la clé (par [CRYPTREC]). Pour plus de considérations sur la sécurité, le lecteur est invité à se reporter à [CRYPTREC], [ISOSEED], et [SEED-EVAL].

7. Considérations relatives l'IANA

L'IANA a alloué l'identifiant de transformation ESP (21) à ESP_SEED_CBC.

8. Remerciements

Les auteurs tiennent à remercier le Docteur Haesuk Kim de Future Systems Inc. et Brian Kim de OULLIM Information Technology Inc. pour leur avis d'expert sur les exemples de valeurs d'essai.

9. Références

9.1 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)

[RFC2406] S. Kent et R. Atkinson, "Encapsulation de charge utile de sécurité IP (ESP)", novembre 1998. *(Ob., voir* RFC4303)

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

[RFC2451] R. Pereira, R. Adams, "Algorithmes de chiffrement ESP en mode CBC", novembre 1998. *(P.S.)*

[RFC4009] J. Park et autres, "Algorithme de chiffrement SEED", février 2005. (*Obsolète, voir* RFC4269) *(Information)*

[TTASSEED] Telecommunications Technology Association (TTA), South Korea, "128-bit Symmetric Block Cipher (SEED)", TTAS.KO- 12.0004, September, 1998 (en coréen) http://www.tta.or.kr/English/new/main/index.htm

9.2 Références pour information

[AES] NIST, FIPS PUB 197, "Advanced Encryption Standard(AES), novembre 2001. http://csrc.nist.gov/publications/fips/fips197/fips-197. {ps,pdf}

[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. "SEED Evaluation Report", février 2002 http://www.kisa.or.kr/seed/seed_eng.html

[ISOSEED] ISO/CEI JTC 1/SC 27 N3979, "Techniques de sécurité des technologies de l'information - Algorithmes de chiffrement - Partie 3 : Chiffrements de blocs", juin 2004.

[MODES] "Symmetric Key Block Cipher Modes of Operation", http://www.nist.gov/modes/ .

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

[RFC2403] C. Madson, R. Glenn, "Utilisation de HMAC-MD5-96 au sein d'ESP et d'AH", novembre 1998. *(P.S.)*

[RFC2404] C. Madson, R. Glenn, "Utilisation de HMAC-SHA-1-96 au sein d'ESP et d'AH", novembre 1998. *(P.S.)*

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

RFC6071)

[SEED-EVAL] KISA, "Self Evaluation Report",
http://www.kisa.or.kr/seed/data/Document_pdf/SEED_Self_Evaluation.pdf"

Adresse des auteurs

Hyangjin Lee
KISA
téléphone : +82-2-405-5446
Fax : +82-2-405-5319
mél : jiinii@kisa.or.kr

Jaeho Yoon
KISA
téléphone : +82-2-405-5434
Fax : +82-2-405-5219
mél : jhyoon@kisa.or.kr

Seoklae Lee
KISA
téléphone : +82-2-405-5230
Fax : +82-2-405-5219
mél : sllee@kisa.or.kr

Jaeil Lee
KISA
téléphone : +82-2-405-5200
Fax : +82-2-405-5219
mél : jilee@kisa.or.kr

Déclaration complète de droits de reproduction

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