Groupe de travail Réseau
Request for Comments : 2405
Catégorie : En cours de normalisation
Traduction Claude Brière de L'Isle

C. Madson, Cisco Systems, Inc.
N. Doraswamy, Bay Networks, Inc.
novembre 1998

Algorithme de chiffrement ESP DES-CBC avec vecteur d'initialisation explicite

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

1. Introduction

Le présent document décrit l'utilisation de l'algorithme de chiffrement DES en mode de chaînage de bloc de chiffrement comme mécanisme de confidentialité dans le contexte de l'encapsulation de charge utile de sécurité.

DES est un algorithme de chiffrement de bloc symétrique. L'algorithme est décrit dans [FIPS-46-2], [FIPS-74], [FIPS-81]. [Schneier96] fournit une description générale du mode de chaînage de bloc de chiffrement, un mode qui est applicable à plusieurs algorithmes de chiffrement.

Comme spécifié dans le présent mémoire, DES-CBC n'est pas un mécanisme d'authentification. (Bien que DES-MAC, décrit dans [Schneier96] entre autres, fournisse l'authentification, DES-MAC n'est pas exposé ici.)

Pour plus d'informations sur la façon dont les diverses pièces de ESP s'accordent ensemble pour fournir des services de sécurité, se reporter à la [RFC2406] et la [RFC2411].

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 et mode

DES-CBC est un algorithme de bloc symétrique à clé secrète. Il a une taille de bloc de 64 bits.

[FIPS-46-2], [FIPS-74] et [FIPS-81] décrivent l'algorithme DES, tandis que [Schneier96] fournit une bonne description du mode CBC.

2.1 Performances

Phil Karn a réglé le logiciel DES-CBC de façon à réaliser 10,45 Mbit/s avec un Pentium à 90 MHz, et 15,9 Mbit/s avec un Pentium à 133 MHz. D'autres estimations de la vitesse de DES se trouvent dans [Schneier96].

3. Charge utile ESP

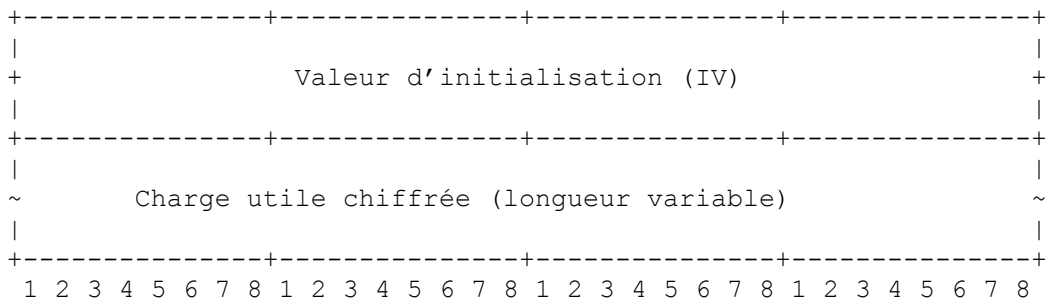
DES-CBC exige une valeur d'initialisation (IV) explicite de 8 octets (64 bits). Cette IV précède immédiatement la charge utile protégée (chiffrée). L'IV DOIT être une valeur aléatoire.

Inclure l'IV dans chaque datagramme assure que le déchiffrement de chaque datagramme reçu peut être effectué, même lorsque certains datagrammes sont abandonnés, ou que des datagrammes sont déclassés dans le transit.

Note de mise en œuvre : la pratique courante est d'utiliser des données aléatoires pour la première IV et les 8 derniers octets de données chiffrées d'un processus de chiffrement comme IV pour le prochain processus de chiffrement ; cela étend logiquement le CBC à travers les paquets. Cela présente aussi l'avantage de limiter les fuites d'informations à partir du générateur de nombres aléatoires. Quel que soit le mécanisme utilisé, le receveur NE DOIT PAS supposer une quelconque signification pour cette valeur, autre que d'être une valeur d'initialisation.

Pour éviter le chiffrement ECB 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 *(nombre de bits différents dans deux blocs de même longueur)* pour les IV.

Le champ Charge utile, comme défini dans la [RFC2406], est coupé selon le diagramme suivant :



3.1 Taille de bloc et bourrage

L'algorithme DES-CBC décrit dans le présent document DOIT utiliser une taille de bloc de 8 octets (64 bits).

Lorsque un bourrage est nécessaire, il DOIT être fait conformément aux conventions spécifiées dans la [RFC2406].

4. Matériel de chiffrement

DES-CBC est un algorithme symétrique à clé secrète. La taille de clé est de 64 bits. (Elle est couramment connue comme clé de 56 bits car la clé a 56 bits significatifs ; le bit de moindre poids de chaque octet est le bit de parité.]

La [RFC2401] décrit le mécanisme général pour déduire le matériel de clé pour la transformation ESP. La déduction de la clé à partir d'une certaine quantité de matériel de clé n'est pas différente dans les associations de sécurité chiffrées manuellement et automatiquement.

Ce mécanisme DOIT déduire une valeur de clé de 64 bits à utiliser par ce chiffrement. Le mécanisme va déduire des valeurs de clé brutes, le processus de déduction lui-même n'étant pas chargé du traitement de parité ou des vérifications de clés faibles.

La vérification de clé faible DEVRAIT être effectuée. Si on trouve une telle clé, elle DEVRAIT être rejetée et une nouvelle SA devrait être demandée.

Note de mise en œuvre : si une mise en œuvre choisit de faire la vérification de clé faible, elle devrait reconnaître que les clés faibles connues [FIPS74] ont été ajustées pour la parité. Autrement, le traitement de la parité est une affaire locale.

Une fonction pseudo-aléatoire forte DOIT être utilisée pour générer la clé demandée. Pour un exposé sur ce sujet, voir la [RFC1750].

4.1 Clés faibles

DES a 16 clés faibles connues, incluant ce qu'on appelle des clé semi-faibles. On trouve la liste des clés faibles dans [FIPS74].

4.2 Durée de vie de clé

[Blaze96] discute des coûts et des temps de récupération de clé pour les attaques en force brute. Il présente diverses combinaisons de coût/temps total pour un rapport clé/coût par clé récupérée pour des clés DES de 40 bits et 56 bits, fondées sur des estimations de fin 1995.

Alors qu'une recherche en force brute d'un espace de clés DES de 56 bits peut être considérée comme infaisable pour le bidouilleur occasionnel, qui utilise simplement les cycles de CPU disponibles ou d'autres ressources à faible coût, elle est à la portée de quelqu'un qui accepte d'y consacrer un peu plus de ressources.

Par exemple, pour un coût de 300 000 $, une clé DES de 56 bits peut être récupérée dans une moyenne de 19 jours en utilisant des technologies en vente libre, et en seulement 3 heures en utilisant un processeur électronique développé spécialement.

On devrait noter qu'il y a d'autres attaques qui peuvent retrouver plus vite la clé, que les attaques en force brute sont considérées comme le "pire des cas", bien que les plus faciles à mettre en œuvre.

[Wiener94] discute aussi d'une machine à 1 million de $ qui peut casser une clé DES en 3,5 heures (estimation de 1993) en utilisant une attaque de texte source connu. Comme exposé dans la section des Considérations sur la sécurité, une attaque de texte source connu est raisonnablement probable.

On devrait aussi noter qu'au fil du temps, les coûts totaux et moyens de recherche ainsi que le temps moyen de récupération de clé vont continuer de diminuer.

Bien que ce qui figure ci-dessus ne fasse pas de recommandations spécifiques sur la durée de vie d'une clé, cela souligne le fait que pour une application donnée, la durée de vie de clé désirée dépend de la menace perçue (un pari risqué sur la quantité de ressources disponible pour l'attaquant) par rapport à la valeur des données à protéger.

Bien qu'on ne fasse ici aucune recommandation sur la durée de vie fondée sur le volume, on devrait noter qu'avec un volume suffisant, il y a une probabilité accrue que du texte source connu puisse être accumulé.

5. Interaction avec les algorithmes d'authentification

Au moment de la rédaction de ce mémoire, il n'y a aucun problème connu qui empêche l'utilisation de l'algorithme DES-CBC avec un algorithme d'authentification quelconque.

6. Considérations sur la sécurité

[La plus grande partie de cette section a été à l'origine écrite par William Allen Simpson et Perry Metzger.]

Les usagers ont besoin de comprendre que la qualité de la sécurité fournie par la présente spécification dépend complètement de la force de l'algorithme DES, de la correction de la mise en œuvre de cet algorithme, de la sécurité du mécanisme de gestion de l'association de sécurité et de sa mise en œuvre, de la force de la clé [CN94], et de la correction de la mise en œuvre dans tous les nœuds participants.

[Bell95] et [Bell96] décrivent une attaque de couper-coller qui s'applique à tous les algorithmes de chaînage de bloc de chiffrement. Cette attaque peut être contrée par l'utilisation d'un mécanisme d'authentification.

L'utilisation d'un mécanisme de chiffrement sans un mécanisme correspondant d'authentification est fortement déconseillée. Ce chiffrement peut être utilisé dans une transformation ESP qui comporte aussi l'authentification ; il peut aussi être utilisé dans une transformation ESP qui ne comporte pas d'authentification pourvu qu'il y ait un en-tête AH qui l'accompagne. Voir les détails dans les [RFC2406], [RFC2402], [RFC2401], et [RFC2411].

Lorsque le bourrage ESP par défaut est utilisé, les octets de bourrage ont une valeur prévisible. Ils fournissent une faible mesure de détection d'altération sur leur propre bloc et le bloc précédent en mode CBC. Cela rend un peu plus difficile

d'effectuer des attaques par découpage, et évite un possible canal couvert. Cette petite quantité de texte source connu ne crée pas de problème aux chiffrements modernes.

Au moment de la rédaction du présent document, [BS93] a démontré une cryptanalyse différentielle fondée sur une attaque de texte source choisi qui exige 2^47 paires de texte source – texte chiffré, où la taille d'une paire est la taille d'un bloc DES (64 bits). [Matsui94] a montré une cryptanalyse linéaire fondée sur une attaque de texte source connu exigeant seulement 2^43 paires de texte source - texte chiffré. Bien que ces attaques ne soient pas considérées comme praticables, elles doivent être prises en considération.

Plus dérangeant, [Wiener94] a montré la conception d'une machine à craquer le DES pour un coût d'un million de dollars qui peut casser une clé toutes les 3,5 heures. Ceci est une attaque extrêmement praticable.

Un ou deux blocs de texte source connu suffisent à retrouver une clé DES. Parce que les datagrammes IP commencent normalement par un bloc de texte d'en-tête connu ou devinable, de fréquents changements de clés ne protègeront pas contre cette attaque.

Il est suggéré que DES n'est pas un bon algorithme de chiffrement pour la protection d'informations de valeur même modérée en face d'un tel équipement. Le triple DES est probablement un meilleur choix à de telles fins.

Cependant, en dépit de ces risques potentiels, le niveau de confidentialité fourni par l'utilisation de l'ESP DES-CBC dans l'environnement de l'Internet est de loin supérieur à l'envoi d'un datagramme en clair.

Le cas de l'utilisation de valeurs aléatoires pour les IV a été précisé avec le résumé suivant fourni par Steve Bellovin. Se reporter à [Bell97] pour plus d'informations.

"Le problème se pose si on utilise un compteur comme IV, ou quelque autre source avec une faible distance de Hamming entre les IV successives pour le chiffrement en mode CBC. En mode CBC, le "texte source efficace" pour un chiffrement est le OUX du texte source réel et le texte chiffré du bloc précédant. Normalement, c'est une valeur aléatoire, ce qui signifie que le texte source efficace est assez aléatoire. Ceci est bien, parce que de nombreux blocs du texte source réel ne changent pas beaucoup non plus d'un paquet à l'autre.

Pour le premier bloc de texte source, la IV prend la place du bloc de texte chiffré précédent. Si la IV ne diffère pas beaucoup de l'IV précédente, et si le bloc de texte source réel ne diffère pas beaucoup de celui du paquet précédent, le texte source efficace ne va pas non plus être très différent. Cela signifie qu'on a des paires de blocs de texte chiffré combinées avec des blocs de texte source qui ne diffèrent que par quelques positions de bits. Cela peut être un biais pour des attaques de cryptanalyse assorties."

La discussion sur les IV a été mise à jour pour exiger qu'une mise en œuvre n'utilise pas une source à faible distance de Hamming pour les IV.

7. Références

[Bell95] Bellovin, S., "An Issue With DES-CBC When Used Without Strong Integrity", Presentation at the 32nd Internet Engineering Task Force, Danvers Massachusetts, avril 1995.

[Bell96] Bellovin, S., "Problem Areas for the IP Security Protocols", Proceedings of the Sixth Usenix Security Symposium, juillet 1996.

[Bell97] Bellovin, S., "Probable Plaintext Cryptanalysis of the IP Security Protocols", Proceedings of the Symposium on Network and Distributed System Security, San Diego, CA, pp. 155-160, février 1997 (ausi à http://www.research.att.com/~smb/papers/probtxt .{ps, pdf}).

[BS93] Biham, E., and A. Shamir, "Differential Cryptanalysis of the Data Encryption Standard", Berlin: Springer-Verlag, 1993.

[Blaze96] Blaze, M., Diffie, W., Rivest, R., Schneier, B., Shimomura, T., Thompson, E., and M. Wiener, "Minimal Key Lengths for Symmetric Ciphers to Provide Adequate Commercial Security", actuellement disponible à http://www.bsa.org/policy/encryption/cryptographers.html .

[CN94] Carroll, J.M., and S. Nudiati, "On Weak Keys and Weak Data: Foiling the Two Nemeses", Cryptologia, Vol. 18, n° 23, pp. 253-280, juillet 1994.

[FIPS-46-2] US National Bureau of Standards, "Data Encryption Standard", Federal Information Processing Standard (FIPS)

Publication 46-2, décembre 1993, http://www.itl.nist.gov/div897/pubs/fip46-2.htm (remplace FIPS-46-1).

[FIPS-74] US National Bureau of Standards, "Guidelines for Implementing and Using the Data Encryption Standard", Federal Information Processing Standard (FIPS) Publication 74, avril 1981, http://www.itl.nist.gov/div897/pubs/fip74.htm .

[FIPS-81] US National Bureau of Standards, "DES Modes of Operation", Federal Information Processing Standard (FIPS) Publication 81, décembre 1980, http://www.itl.nist.gov/div897/pubs/fip81.htm .

[Matsui94] Matsui, M., "Linear Cryptanalysis method for DES Cipher", Advances in Cryptology -- Eurocrypt '93 Proceedings, Berlin: Springer-Verlag, 1994.

[RFC1750] D. Eastlake 3rd et autres, "Recommandations d'aléa pour la sécurité", décembre 1994. *(Info., remplacée par la* RFC4086)

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

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

[RFC2402] S. Kent et R. Atkinson, "En-tête d'authentification IP", novembre 1998. (*Obsolète, voir* RFC4302, 4305)

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

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

[Schneier96] Schneier, B., "Applied Cryptography Second Edition", John Wiley & Sons, New York, NY, 1996. ISBN 0-471-12845-7.

[Wiener94] Wiener, M.J., "Efficient DES Key Search", School of Computer Science, Carleton University, Ottawa, Canada, TR-244, mai 1994. Présenté à la Rump Session de Crypto '93. [Republié dans "Practical Cryptography for Data Internetworks", W.Stallings, éditeur, IEEE Computer Society Press, pp.31-79 (1996). Actuellement disponible à ftp://ripem.msu.edu/pub/crypt/docs/des-key-search.ps .]

8. Remerciements

Beaucoup des informations présentées ici ont leur origine dans divers documents ESP-DES dont l'auteur est Perry Metzger et William Allen Simpson, en particulier la section Considérations sur la sécurité.

Le présent document est aussi dérivé en partie de travaux antérieurs de Jim Hughes, et les gens qui ont travaillé avec Jim sur les transformations combinées de ESP DES-CBC+HMAC-MD5, les participants à la réunion ANX, et les membres du groupe de travail IPsec.

Merci à Rob Glenn pour son assistance dans le formatage nroff.

Le groupe de travail IPSec peut être contacté via la liste de diffusion du groupe de travail IPSec à (ipsec@tis.com) ou par ses présidents :

Robert Moskowitz
International Computer Security Association
mél : rgm@icsa.net

Theodore Y. Ts'o
Massachusetts Institute of Technology
mél : tytso@MIT.EDU

9. Adresses des éditeurs

Cheryl Madson
Cisco Systems, Inc.
mél : cmadson@cisco.com

Naganand Doraswamy
Bay Networks, Inc.
mél : naganand@baynetworks.com

10. Déclaration complète de droits de reproduction

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