Groupe de travail Réseau
Request for Comments : 1829
Catégorie : En cours de normalisation
Traduction Claude Brière de L'Isle

P. Karn, Qualcomm
P. Metzger, Piermont
W. Simpson, Daydreamer
août 1995

Transformation ESP DES-CBC

Résumé
Le présent document décrit la transformation de sécurité DES-CBC pour l'encapsulation dans IP de la charge utile de sécurité (ESP).

Table des Matières

1. Introduction

L'encapsulation de charge utile de sécurité (ESP) [RFC1827] assure la confidentialité des datagrammes IP en chiffrant les données de la charge utile à protéger. La présente spécification décrit l'utilisation par ESP du mode de chaînage de bloc de chiffrement (CBC, *Cipher Block Chaining*) de l'algorithme de la norme US de chiffrement des données (DES, *Data Encryption Standard*) [FIPS-46], [FIPS-46-1], [FIPS-74], [FIPS-81].

Toutes les mises en œuvre qui revendiquent la conformité ou la compatibilité avec la spécification d'encapsulation de charge utile de sécurité DOIVENT mettre en œuvre la présente transformation DES-CBC.

Le présent document suppose que le lecteur est familiarisé avec le document "Architecture de sécurité pour le protocole Internet" [RFC1825], qui définit le plan global de sécurité pour IP, et constitue le fondement le plus important de la présente spécification.

1.1 Clés

La clé secrète DES partagée entre les parties à la communication est long de huit octets. Cette clé consiste en une quantité de 56 bits utilisée par l'algorithme DES. La clé de 56 bits est mémorisée comme une quantité de 64 bits (huit octets) avec le bit de moindre poids de chaque octet utilisé comme bit de parité.

1.2 Vecteur d'initialisation

Ce mode de DES exige un vecteur d'initialisation (IV) long de huit octets.

Chaque datagramme contient son propre IV. Inclure l'IV dans chaque datagramme assure que le déchiffrement de chaque

datagramme reçu peut être effectué, même lorsque d'autres datagrammes ont été éliminés, ou que des datagrammes sont réarrangés dans le transit.

La méthode de choix des valeurs d'IV dépend de la mise en œuvre.

Note : Une technique courante acceptable est un simple compteur, qui commence à une valeur choisie au hasard. Alors que cela fournit une méthode aisée pour empêcher la répétition, et que c'est suffisamment robuste pour une utilisation pratique, l'analyse cryptographique peut utiliser les rares occurrences occasionnelles où une position binaire correspondante dans le premier bloc DES s'incrémente exactement de la même façon. D'autres mises en œuvre assurent l'imprévisibilité, habituellement grâce à un générateur de nombres pseudo aléatoires. Il faut veiller à ce que la périodicité du générateur de nombre soit assez longue pour empêcher la répétition durant la durée de vie de la clé de la clé de session.

1.3 Taille des données

L'algorithme DES fonctionne sur des blocs de huit octets. Cela oblige souvent à un bourrage après la fin des données de la charge utile non chiffrée.

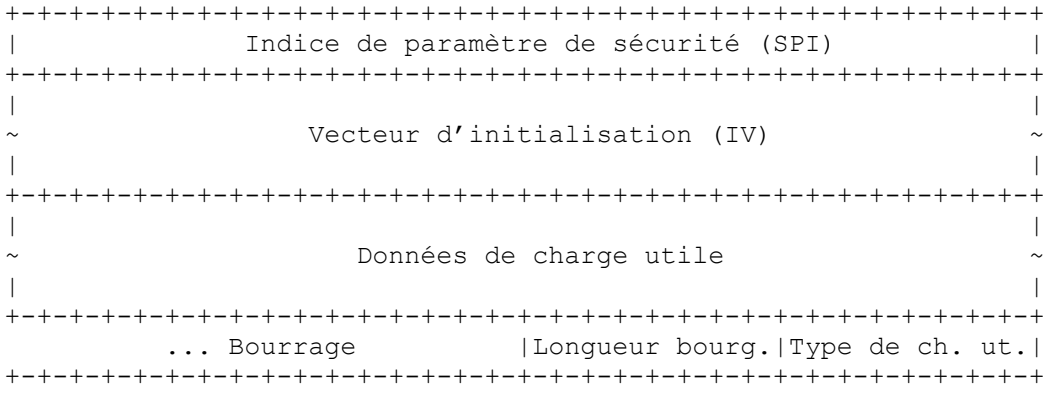
L'entrée et la sortie résultent toutes deux en le même nombre d'octets, ce qui facilite le chiffrement et le déchiffrement en place.

À réception, si la longueur des données à déchiffrer n'est pas un multiple entier de huit octets, une erreur est alors indiquée, comme décrit dans la [RFC1825].

1.4 Performances

Au moment de la rédaction, au moins une mise en œuvre de matériel peut chiffrer ou déchiffrer environ 1 Gbit/s [Schneier94, p. 231].

2. Format de charge utile



Indice de paramètre de sécurité (SPI)
Valeur de 32 bits qui identifie les paramètres de sécurité pour ce datagramme. La valeur NE DOIT PAS être zéro.

Vecteur d'initialisation (IV)
La taille de ce champ est variable, bien qu'elle soit constante pour tous les datagrammes DES-CBC de même SPI et destination IP. Les octets sont envoyés dans l'ordre des octets du réseau (octet de poids fort en premier) [RFC1700]. La taille DOIT être un multiple de 32 bits. Les tailles de 32 et 64 bits sont obligatoirement prises en charge. L'utilisation d'autres tailles sort du domaine d'application de la présente spécification. La taille est supposée être indiquée par le mécanisme de gestion de clé. Lorsque la taille est 32 bits, un IV de 64 bits est formé à partir de la valeur de 32 bits suivie par (enchaînée avec) le complément au bit près de la valeur de 32 bits. Cette taille de champ est très courante, car elle aligne les données de charge utile pour les traitement aussi bien sur 32 que sur 64 bits. Toutes les mises en œuvre conformes DOIVENT aussi traiter correctement une taille de champ de 64 bits. Cela assure une stricte compatibilité avec les mises en œuvre de matériels existantes. Il est prévu que la valeur ne se répète pas durant la durée de vie de la clé de chiffrement de session. Même lorsque un IV complet de 64 bits est utilisé, la clé de session DEVRAIT être changée au moins tous les 2**32 datagrammes.

Données de charge utile
La taille de ce champ est variable. Avant le chiffrement et après le déchiffrement, ce champ commence par l'en-tête Protocole/charge utile IP spécifié dans le champ Type de charge utile. Noter que dans le cas d'encapsulation IP dans IP (Type de charge utile 4) ce sera un autre en-tête IP.

Bourrage
La taille de ce champ est variable. Avant le chiffrement, il est rempli par des valeurs non spécifiées qui dépendent de la mise en œuvre (de préférence, aléatoires) pour aligner les champs Longueur de bourrage et Type de charge utile sur une limite de huit octets. Après déchiffrement, il DOIT être ignoré.

Longueur de bourrage
Ce champ indique la taille du champ Bourrage. Il n'inclut pas les champs Longueur de bourrage et Type de charge utile. La valeur est normalement dans la gamme de 0 à 7, mais peut aller jusqu'à 255 pour permettre de cacher la longueur réelle des données. Ce champ est opaque. C'est-à-dire que la valeur est établie avant le chiffrement, et n'est examinée qu'après le déchiffrement.

Type de charge utile
Ce champ indique le contenu du champ Données de charge utile, en utilisant la valeur de Protocole/charge utile IP. Les valeurs à jour de Protocole/charge utile IP sont spécifiées dans la plus récente version des "Numéros alloués" [RFC1700]. Ce champ est opaque. C'est-à-dire que la valeur est établie avant le chiffrement, et n'est examinée qu'après le déchiffrement. Par exemple, lors du chiffrement d'un datagramme IP entier (en mode tunnel) ce champ contiendra la valeur 4, qui indique l'encapsulation IP dans IP.

3. Algorithme

En DES-CBC, la fonction de chiffrement DES de base est appliquée au OUX de chaque bloc de texte en clair avec le bloc de texte chiffré précédent pour donner le texte chiffré pour le bloc en cours. Cela assure la re-synchronisation lorsque des datagrammes sont perdus.

Pour plus d'explications et des informations mise en œuvre de DES, voie [Schneier94].

3.1 Chiffrement

Ajouter zéro, un ou plusieurs octets (de préférence, un nombre aléatoire) de bourrage au texte en clair, pour rendre sa longueur modulo 8 égale à 6. Par exemple, si la longueur du texte en clair est 41, on ajoutera 5 octets de bourrage.

Ajouter un octet longueur de bourrage contenant le nombre d'octets de bourrage juste ajoutés.

Ajouter un octet type de charge utile contenant la valeur de protocole/charge utile IP qui identifie l'en-tête de protocole qui commence la charge utile.

Fournir un vecteur d'initialisation (IV) de la taille indiquée par le SPI.

Chiffrer la charge utile avec DES en mode CBC, produisant un texte chiffré de la même longueur.

Les octets sont transposés en blocs DES dans l'ordre des octets du réseau (octet de poids fort en premier) [RFC1700]. L'octet 0 (modulo 8) de la charge utile correspond aux bits 1 à 8 du bloc d'entrée DES de 64 bits, tandis que l'octet 7 (modulo 8) correspond aux bits 57 à 64 du bloc d'entrée DES.

Construire un datagramme IP approprié pour la destination cible, avec les SPI, IV, et charge utile indiqués.

La longueur total/charge utile dans l'en-tête IP encapsulant reflète la longueur des données chiffrées, plus les octets de SPI, IV, bourrage, longueur de bourrage, et type de charge utile.

3.2 Déchiffrement

D'abord, le champ SPI est retiré et examiné. Il est utilisé comme un indice dans le tableau local des paramètres de sécurité pour trouver les paramètres négociés et la clé de déchiffrement.

La forme négociée de l'IV détermine la taille du champ IV. Ces octets sont retirés, et une valeur d'IV de 64 bits appropriée

est construite.

La partie chiffrée de la charge utile est déchiffrée en utilisant DES en mode CBC.

Le type de charge utile est retiré et examiné. Si il n'est pas reconnu, la charge utile est éliminée avec un message approprié.

La longueur de bourrage est retirée et examinée. Le nombre spécifié d'octets de bourrage est retiré de la fin de la charge utile déchiffrée, et la longueur totale/charge utile IP est ajustée en conséquence.

Le ou les en-têtes IP et la portion restante de la charge utile déchiffrée sont passés au sous-programme de réception du protocole spécifié dans le champ Type de charge utile.

Considérations pour la sécurité

Les utilisateurs doivent 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 clé et de sa mise en œuvre, de la force de la clé [CN94], et de la correction des mises en œuvre de tous les nœuds participants.

Entre autres considérations, les applications peuvent veiller à ne pas choisir des clés faibles, bien que le risque d'en tirer une au hasard soit faible [Schneier94, p 233].

L'attaque par coupé collé décrite par [Bell95] exploite la nature de tous les algorithmes de chaînage de bloc de chiffrement. Lorsque un bloc est endommagé dans la transmission, lors du déchiffrement, lui et les blocs suivants seront mélangés par le processus de déchiffrement, mais tous les blocs suivants seront déchiffrés correctement. Si un attaquant a un accès légitime à la même clé, cette caractéristique peut être utilisée pour insérer ou répéter des données précédemment chiffrées d'autres utilisateurs du même moteur, ce qui révèle le texte en clair. La somme de contrôle de transport usuelle (ICMP, TCP, UDP) peut détecter cette attaque, mais par elle même, elle n'est pas considérée comme cryptographiquement forte. Dans cette situation, une vérification de l'usager ou de la connexion est nécessaire [RFC1826].

Au moment de la rédaction du présent document, [BS93] a démontré une attaque de texte en clair choisi fondée sur une analyse cryptographique différentielle exigeant 2^47 paires de texte en clair-texte chiffré, et [Matsui94] démontre une attaque de texte en clair connu fondée sur une analyse cryptographique linéaire exigeant seulement 2^43 paires de texte en clair-texte chiffré. Bien que ces attaques ne soient pas considérées comme praticables, elles doivent être prises en compte.

Plus dérangeant, [Weiner94] a montré que la conception d'une machine à casser un DES coûterait 1 million de dollars et pourrait casser une clé en 3,5 heures. Ceci est une attaque extrêmement praticable.

Un ou deux blocs de texte en clair connus suffisent pour récupérer une clé DES. Comme les datagrammes IP commencent normalement par un bloc d'en-tête connu et/ou devinable, des changements de clé fréquents ne vont pas protéger contre cette attaque.

Il est suggéré que DES n'est pas un bon algorithme de chiffrement pour la protection d'informations même de valeur modérée en face de tels équipements. Le Triple DES est probablement un meilleur choix pour un tel objet.

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

Remerciements

Le présent document a été relu par le groupe de travail Sécurité IP de l'équipe d'ingénierie de l'Internet (IETF). Les commentaires devraient être soumis à la liste de diffusion <ipsec@ans.net>.

Une partie du texte de la présente spécification a été empruntée au travail de Randall Atkinson pour les groupes de travail SIP, SIPP, et IPv6.

L'utilisation de DES pour la confidentialité est étroitement modelée sur le travail réalisé pour SNMPv2 [RFC1446].

Steve Bellovin, Steve Deering, Karl Fox, Charles Lynn, Craig Metz, Dave Mihelcic et Jeffrey Schiller ont fourni d'utiles critiques sur les premières versions de ce document.

Références

[Bell95] Bellovin, S., "An Issue With DES-CBC When Used Without Strong Integrity", Compte-rendu de la 32ème réunion de l'IETF, Danvers, MA, avril 1995.

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

[CN94] Carroll, J.M., and Nudiati, S., "On Weak Keys and Weak Data: Foiling the Two Nemeses", Cryptologia, Vol. 18 No. 23 pp. 253-280, juillet 1994.

[FIPS-46] US National Bureau of Standards, "Data Encryption Standard", Federal Information Processing Standard (FIPS) Publication 46, janvier 1977.

[FIPS-46-1] US National Bureau of Standards, "Data Encryption Standard", Federal Information Processing Standard (FIPS) Publication 46-1, janvier 1988.

[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.

[FIPS-81] US National Bureau of Standards, "DES Modes of Operation" Federal Information Processing Standard (FIPS) Publication 81, décembre 1980.

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

[RFC1446] J. Galvin et K. McCloghrie, "Protocoles de sécurité pour la version 2 de SNMP", avril 1993. *(Historique)*

[RFC1700] J. Reynolds et J. Postel, "Numéros alloués", STD 2, octobre 1994. *(Historique, voir www.iana.org))*

[RFC1800] J. Postel, éd., "Normes officielles de protocole de l'Internet", juillet 1995. *(Obsolète, voir* RFC1880*) (Historique)*

[RFC1825] R. Atkinson, "Architecture de sécurité pour le protocole Internet", août 1995. *(Obsolète, voir* RFC2401*)*

[RFC1826] R. Atkinson, "En-tête d'authentification IP", août 1995. *(Obsolète, voir la* RFC2402*)*

[RFC1827] R. Atkinson, "Encapsulation dans IP de charge utile de sécurité (ESP)", août 1995. *(Obsolète, voir* RFC2406*)*

[Schneier94] Schneier, B., "Applied Cryptography", John Wiley & Sons, New York, NY, 1994. ISBN 0-471-59756-2

[Weiner94] Wiener, M.J., "Efficient DES Key Search", School of Computer Science, Carleton University, Ottawa, Canada, TR-244, mai 1994. Présenté à la session finale de Crypto '93.

Adresse des auteurs

Les questions sur le présent mémoire peuvent être envoyées à :

Phil Karn
Qualcomm, Inc.
6455 Lusk Blvd.
San Diego, California 92121-2779
karn@unix.ka9q.ampr.org

Perry Metzger
Piermont Information Systems Inc.
160 Cabrini Blvd., Suite #2
New York, NY 10033
perry@piermont.com

William Allen Simpson
Daydreamer
Computer Systems Consulting Services
1384 Fontaine
Madison Heights, Michigan 48071
Bill.Simpson@um.cc.umich.edu
bsimpson@MorningStar.com