Groupe de travail Réseau
Request for Comments : 2947
Catégorie : En cours de normalisation

J. Altman, Columbia University
September 2000
Traduction Claude brière de L'Isle

Chiffrement Telnet : DES3 en chiffrement à rebouclage par le chiffre à 64 bits

Résumé
Le présent document spécifie comment utiliser l'algorithme de chiffrement triple-DES (norme de chiffrement des données) en mode à rebouclage par le chiffre avec l'option de chiffrement Telnet.

1. Noms et codes des commandes

Type de chiffrement

DES3_CFB64 3

Commandes de sous-option

CFB64_IV 1
CFB64_IV_OK 2
CFB64_IV_BAD 3

2. Signification des commandes

IAC SB ENCRYPT IS DES3_CFB64 CFB64_IV <vecteur initial> IAC SE
L'envoyeur de cette commande génère un vecteur initial aléatoire de 8 octets, et l'envoie à l'autre côté de la connexion en utilisant la commande CFB64_IV. Le vecteur initial est envoyé en clair. Seul le côté de la connexion qui est WILL ENCRYPT peut envoyer la commande CFB64_IV.

IAC SB ENCRYPT REPLY DES3_CFB64 CFB64_IV_OK IAC SE
IAC SB ENCRYPT REPLY DES3_CFB64 CFB64_IV_BAD IAC SE
L'envoyeur de ces commandes accepte ou rejette le vecteur initial reçu dans une commande CFB64_IV. Seul le côté de la connexion qui est DO ENCRYPT peut envoyer les commandes CFB64_IV_OK et CFB64_IV_BAD. La commande CFB64_IV_OK DOIT être envoyée pour la rétro compatibilité avec les mises en œuvre existantes ; il n'y a en fait aucune raison pour qu'un envoyeur ait besoin d'envoyer la commande CFB64_IV_BAD sauf dans le cas d'une violation du protocole où le vecteur initial envoyé ne serait pas de longueur correcte (c'est-à-dire pas de 8 octets).

3. Règles de mise en œuvre

Une fois qu'une commande CFB64_IV_OK a été reçue, le côté WILL ENCRYPT de la connexion devrait faire une négociation d'id_de_clé en utilisant la commande ENC_KEYID. Une fois que la négociation de id_de_clé a bien identifié un id_de_clé commun, les commandes START et END peuvent alors être envoyées par le côté de la connexion qui est WILL ENCRYPT. Les données seront chiffrées en utilisant l'algorithme de rétroaction DES3 à 64 bits.

Si le chiffrement (déchiffrement) est désactivé et réactivé à nouveau, et si le même id_de_clé est utilisé lors du redémarrage du chiffrement (déchiffrement) le texte en clair qui intervient ne doit pas changer l'état de la machine de chiffrement (déchiffrement).

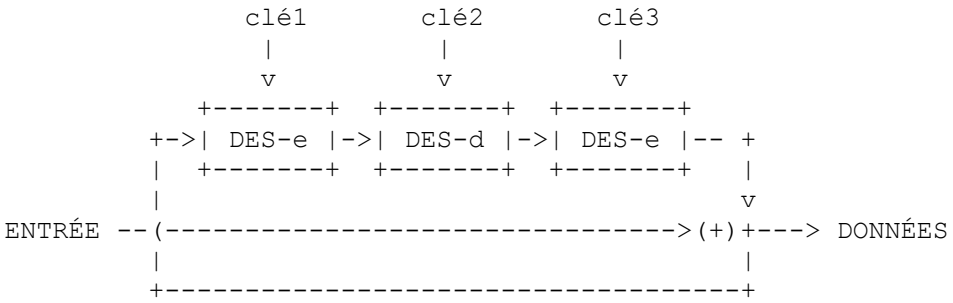
Si une commande START est envoyée (reçue) avec un id_de_clé différent, la machine de chiffrement (déchiffrement) doit être réinitialisée immédiatement après la fin de la commande START avec la nouvelle clé et le vecteur initial envoyés (reçus) dans la dernière commande CFB64_IV.

Si une nouvelle commande CFB64_IV est envoyée (reçue) et si le chiffrement (déchiffrement) est activé, la machine de chiffrement (déchiffrement) doit être réinitialisée immédiatement après la fin de la commande CFB64_IV avec le nouveau vecteur initial et le id_de_clé envoyés (reçus) dans la dernière commande START.

Si le chiffrement (déchiffrement) n'est pas activé lorsque une commande CFB64_IV est envoyée (reçue) la machine de chiffrement (déchiffrement) doit être réinitialisée après la prochaine commande START, avec le id_de_clé envoyé (reçu) dans cette commande START, et le vecteur initial envoyé (reçu) dans cette commande CFB64_IV.

4. Algorithme

Rétroaction de chiffrement DES3 à 64 bits



Sachant que :

iV : vecteur initial, est long de 64 bits (8 octets).
Dn : est le n^{e} tronçon de 64 bits (8 octets) de données à chiffrer (déchiffrer).
On : est le n^{e} tronçon de 64 bits (8 octets) de résultat chiffré (déchiffré).
V0 = DES-e(DES-d(DES-e(iV, clé1),clé2),clé3)
On = Dn ^ Vn
V(n+1) = DES-e(DES-d(DES-e(On, clé1),clé2),clé3)

5. Intégration avec l'option Telnet AUTHENTICATION

Comme noté dans la spécification de l'option Telnet ENCRYPTION, une valeur de id_de_clé de zéro indique la clé de chiffrement par défaut, qui peut être déduite de l'option Telnet AUTHENTICATION. Si la clé de chiffrement par défaut négociée parce que l'option Telnet AUTHENTICATION contient moins de 16 octets, l'option DES3_CFB64 ne doit alors pas être offerte ou utilisée comme option de chiffrement Telnet valide.

Les règles suivantes sont à suivre pour créer les clés de chiffrement DES3 sur la base des données de chiffrement disponibles:

clés_à_utiliser = octets de données de clés / taille de bloc DES (8 octets)

où les clés sont étiquetées de "clé1" à "clé6" avec "clé1" comme 8 premiers octets ; "clé2" les 8 octets suivants; ... et "clé6" étant le sixième groupe de 8 octets (si disponible).

Lorsque deux clés sont disponibles :

. les données envoyées du serveur sont chiffrées avec clé1, déchiffrées avec clé2, et chiffrées avec clé1 ;

. les données envoyées du client sont chiffrées avec clé2, déchiffrées avec clé1, et chiffrées avec clé2

Lorsque trois clés sont disponibles :

. les données envoyées du serveur sont chiffrées avec clé1, déchiffrées avec clé2, et chiffrées avec clé3 ;

. les données envoyées du client sont chiffrées avec clé2, déchiffrées avec clé3, et chiffrées avec clé1

Lorsque quatre clés sont disponibles :

. les données envoyées du serveur sont chiffrées avec clé1, déchiffrées avec clé2, et chiffrées avec clé3 ;

. les données envoyées du client sont chiffrées avec clé2, déchiffrées avec clé4, et chiffrées avec clé1

Lorsque cinq clés sont disponibles :

. les données envoyées du serveur sont chiffrées avec clé1, déchiffrées avec clé2, et chiffrées avec clé3 ;

. les données envoyées du client sont chiffrées avec clé2, déchiffrées avec clé4, et chiffrées avec clé5

Lorsque six clés sont disponibles :

. les données envoyées du serveur sont chiffrées avec clé1, déchiffrées avec clé2, et chiffrées avec clé3 ;

. les données envoyées du client sont chiffrées avec clé4, déchiffrées avec clé5, et chiffrées avec clé6

Dans tous les cas, les clés utilisées par DES3_CFB64 doivent avoir leur parité corrigée après qu'il est déterminé qu'elles utilisent l'algorithme ci-dessus.

Noter que l'algorithme ci-dessus suppose qu'il est sûr d'utiliser une clé non DES (ou une partie d'une clé non DES) comme une clé DES. Ce n'est pas nécessairement vrai de tous les systèmes de chiffrement, mais on spécifie ce comportement comme comportement par défaut car il est vrai pour la plupart des systèmes d'authentification d'utilisation courante aujourd'hui, et pour la compatibilité avec les mises en œuvre existantes. De nouveaux mécanismes AUTHENTICATION Telnet pourront spécifier des méthodes de remplacement pour déterminer les clés à utiliser pour cette suite de chiffrement dans leur spécification, si la clé de session négociée par ce mécanisme d'authentification n'est pas une clé DES et lorsque cet algorithme peut n'être pas d'utilisation sûre.

6. Considérations pour la sécurité

Le chiffrement fait à l'aide de la rétroaction de chiffrement n'assure pas l'intégrité des données ; l'attaquant actif a une capacité limitée à modifier le texte, si il peut prédire le texte en clair qui a été transmis. Les limitations auxquelles fait face l'attaquant (le fait que seulement 8 octets peuvent être modifiés à la fois, et que le bloc de données de 8 octets suivant sera corrompu, ce qui rend la détection vraisemblable) sont significatives, mais il est possible qu'un attaquant actif puisse quand même être capable d'exploiter cette faiblesse.

Le compromis est ici que d'ajouter un code d'authentification de message (MAC) va augmenter de façon significative le nombre d'octets nécessaire pour envoyer un seul caractère dans le protocole Telnet, ce qui va impacter les performances sur les liaisons lentes (c'est-à-dire, téléphoniques).

7. Remerciements

Le présent document se fonde sur le document "Telnet Encryption : DES 64 bit Cipher Feedback" rédigé à l'origine par Dave Borman de Cray Research avec l'assistance du groupe de travail Telnet de l'IETF.

Adresse de l'auteur

Jeffrey Altman, Editor
Columbia University
612 West 115th Street Room 716
New York NY 10025
USA
téléphone : +1 (212) 854-1344
mél : jaltman@columbia.edu

Déclaration complète de droits de reproduction

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