

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

### Statut du présent mémoire

Le présent document spécifie un protocole de l'Internet en cours de normalisation pour la communauté de l'Internet, et appelle à des discussions et suggestions pour son amélioration. Prière de se référer à l'édition en cours des "Normes officielles des protocoles de l'Internet" (STD 1) pour connaître l'état de la normalisation et le statut de ce protocole. La distribution du présent mémoire n'est soumise à aucune restriction.

### Notice de Copyright

Copyright (C) The Internet Society (2000). Tous droits réservés.

### 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'expéditeur 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'expéditeur 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 expéditeur 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).

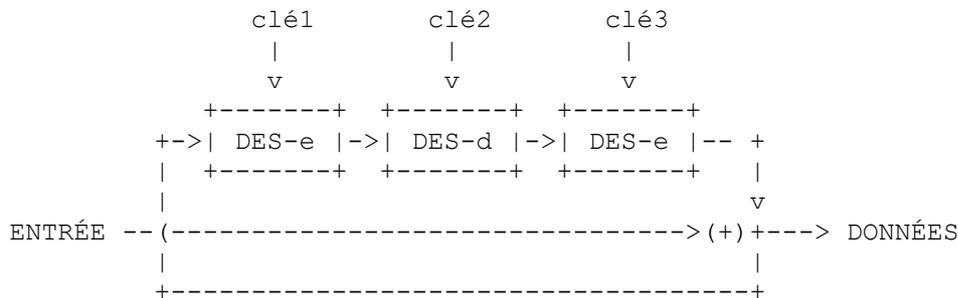
Si une commande START est envoyée (reçue) avec un id\_de\_clé différent, la machine de chiffrement (déchiffrement) doit être réinitialisée immédiatement après la fin de la commande START avec la nouvelle clé et le vecteur initial envoyés (reçus) dans la dernière commande CFB64\_IV.

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<sup>e</sup> tronçon de 64 bits (8 octets) de données à chiffrer (déchiffrer).

On : est le n<sup>e</sup> 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**

Copyright (C) The Internet Society (2000). Tous droits réservés.

Ce document et les traductions de celui-ci peuvent être copiés et diffusés, et les travaux dérivés qui commentent ou expliquent autrement ou aident à sa mise en œuvre peuvent être préparés, copiés, publiés et distribués, partiellement ou en totalité, sans restriction d'aucune sorte, à condition que l'avis de droits de reproduction ci-dessus et ce paragraphe soient inclus sur toutes ces copies et œuvres dérivées. Toutefois, ce document lui-même ne peut être modifié en aucune façon, par exemple en supprimant le droit d'auteur ou les références à l'Internet Society ou d'autres organisations Internet, sauf si c'est nécessaire à l'élaboration des normes Internet, auquel cas les procédures pour les droits de reproduction définies dans les processus des normes de l'Internet doivent être suivies, ou si nécessaire pour le traduire dans des langues autres que l'anglais.

Les permissions limitées accordées ci-dessus sont perpétuelles et ne seront pas révoquées par la Société Internet ou ses successeurs ou ayants droit.

Ce document et les renseignements qu'il contient sont fournis "TELS QUELS" et l'INTERNET SOCIETY et l'INTERNET ENGINEERING TASK FORCE déclinent toute garantie, expresse ou implicite, y compris mais sans s'y limiter, toute garantie que l'utilisation de l'information ici présente n'enfreindra aucun droit ou aucune garantie implicite de commercialisation ou d'adaptation à un objet particulier.

### **Remerciement**

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