

Groupe de travail Réseau  
**Request for Comments : 2953**  
Catégorie : Information

T. Ts'o, VA Linux Systems  
septembre 2000  
Traduction Claude Brière de L'Isle

## Chiffrement Telnet : DES en chiffrement à rebouclage par la sortie à 64 bits

### Statut de ce mémoire

Le présent mémoire apporte des informations pour la communauté de l'Internet. Il ne spécifie aucune norme de l'Internet. La distribution du présent mémoire n'est soumise à aucune restriction.

### Copyright Notice

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

### Résumé

Le présent document spécifie comment utiliser l'algorithme de chiffrement de la norme de chiffrement des données (DES) en mode à rebouclage de sortie avec l'option de chiffrement Telnet.

## 1. Noms et codes des commandes

Type de chiffrement

DES\_OFB64 2

Commandes de sous-option

OFB64\_IV 1

OFB64\_IV\_OK 2

OFB64\_IV\_BAD 3

## 2. Signification des commandes

IAC SB ENCRYPT IS DES\_OFB64 OFB64\_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 OFB64\_IV. Le vecteur initial est envoyé en clair. Seul le côté de la connexion qui est WILL ENCRYPT peut envoyer la commande OFB64\_IV.

IAC SB ENCRYPT REPLY DES\_OFB64 OFB64\_IV\_OK IAC SE

IAC SB ENCRYPT REPLY DES\_OFB64 OFB64\_IV\_BAD IAC SE

L'expéditeur de ces commandes accepte ou rejette le vecteur initial reçu dans une commande OFB64\_IV. Seul le côté de la connexion qui est DO ENCRYPT peut envoyer les commandes OFB64\_IV\_OK et OFB64\_IV\_BAD. La commande OFB64\_IV\_OK DOIT être envoyée pour la rétro compatibilité avec les mises en œuvre existantes ; il n'y a aucune raison pour qu'un expéditeur ait besoin d'envoyer la commande OFB64\_IV\_BAD sauf dans le cas d'une violation de protocole où le vecteur initial envoyé n'aurait pas la longueur correcte (c'est à dire, ne ferait pas 8 octets).

## 3. Règles de mise en œuvre

Une fois qu'une commande OFB64\_IV\_OK a été reçue, le côté WILL ENCRYPT de la connexion devrait faire la négociation d'id\_de\_clé en utilisant la commande ENC\_KEYID. Une fois que la négociation du 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 DES à rebouclage par la sortie 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 OFB64\_IV.

Si une nouvelle commande OFB64\_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 OFB64\_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 OFB64\_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 OCFB64\_IV.

#### 4. Algorithme

Sachant que  $V[i]$  est le vecteur initial de 64 bits,  $V[n]$  est le  $n^{\text{e}}$  vecteur de 64 bits,  $D[n]$  est le  $n^{\text{e}}$  tronçon de 64 bits de données à chiffrer (déchiffrer), et  $O[n]$  est le  $n^{\text{e}}$  tronçon de 64 bits de données chiffrées (déchiffrées), alors :

$$\begin{aligned} V[0] &= \text{DES}(V[i], \text{clé}) \\ V[n+1] &= \text{DES}(V[n], \text{clé}) \\ O[n] &= D[n] \text{ <OU exclusif> } V[n] \end{aligned}$$

#### 5. Intégration avec l'option telnet AUTHENTICATION

Comme il est noté dans les spécifications de l'option Telnet ENCRYPTION, une valeur d'id\_de\_clé de zéro indique la clé de chiffrement par défaut, comme on peut la déduire de l'option Telnet AUTHENTICATION. Si la clé de chiffrement par défaut négociée par suite de l'option Telnet AUTHENTICATION contient moins de 8 octets, l'option DES\_OFB64 ne doit alors pas être offerte ni utilisée comme option de chiffrement Telnet valide. Si la clé de chiffrement négociée par suite de l'option Telnet AUTHENTICATION fait plus de 16 octets, les huit premiers octets de la clé devraient être utilisés comme id\_de\_clé 0 pour les données envoyées du client Telnet au serveur Telnet, et les huit octets suivants de la clé devraient être utilisés comme id\_de\_clé 0 pour les données envoyées par le serveur Telnet au client Telnet. Autrement, les huit premiers octets de la clé de chiffrement sont utilisés comme id\_de\_clé zéro pour l'option Telnet ENCRYPTION dans les deux directions (avec le client comme WILL ENCRYPT et le serveur comme WILL ENCRYPT).

Dans tous les cas, si la clé négociée par l'option Telnet AUTHENTICATION n'était pas une clé DES, la clé utilisée par le DES\_OFB64 doit avoir sa parité corrigée après qu'il a été déterminé d'utiliser 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. Ceci n'est pas nécessairement vrai de tous les systèmes de chiffrement, mais on spécifie ce comportement comme le 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 d'authentification Telnet pourront spécifier d'autres méthodes pour déterminer dans leur spécification les clés à utiliser pour cette suite de chiffrement, 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 utilisé de façon sûre.

#### 6. Considérations pour la sécurité

Le chiffrement fait à l'aide du rebouclage de sortie n'assure pas de l'intégrité des données ; un attaquant actif peut être capable de substituer du texte, si il peut prédire le texte en clair qui a été transmis. Pour cette raison, le type de chiffrement par rebouclage du chiffre devrait être plutôt utilisé car il fournit une capacité de détection limitée de la modification des données. Aucu des deux ne fournit cependant une vrai protection de l'intégrité des données.

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

## 7. Remerciements

Ce document a été rédigé à l'origine par Dave Borman de Cray Research avec le concours du groupe de travail Telnet de l'IETF.

### Adresse de l'auteur

Theodore Ts'o  
VA Linux Systems  
43 Pleasant St.  
Medford, MA 02155  
USA  
téléphone : (781) 391-3464  
mél : tytso@mit.edu

## 8 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.