Groupe de travail Réseau
Request for Comments : 2950
Catégorie : En cours de normalisation

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

Chiffrement Telnet : CAST-128 en rebouclage de chiffrement à 64 bits

Résumé
Le présent document spécifie comment utiliser l'algorithme de chiffrement CAST-128 en mode à rebouclage de chiffrement avec l'option de chiffrement telnet. Deux tailles de clés sont définies : 40 bits et 128 bits.

1. Noms et codes des commandes

Type de chiffrement

CAST5_40_CFB64	8
CAST128_CFB64	10

Commandes de sous-option

CFB64_IV	1
CFB64_IV_OK	2
CFB64_IV_BAD	3

2. Signification des commandes

IAC SB ENCRYPT IS CAST5_40_CFB64 CFB64_IV <vecteur initial> IAC SE
IAC SB ENCRYPT IS CAST128_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 CAST5_40_CFB64 CFB64_IV_OK IAC SE
IAC SB ENCRYPT REPLY CAST128_CFB64 CFB64_IV_OK IAC SE
IAC SB ENCRYPT REPLY CAST5_40_CFB64 CFB64_IV_BAD IAC SE
IAC SB ENCRYPT REPLY CAST128_CFB64 CFB64_IV_BAD IAC SE
L'envoyeur de ces commande 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 aen fait aucune raison 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 ferait pas la longueur correcte (c'est à dire, ne ferait pas 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 de 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 CAST128 de rebouclage par le chiffre 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).

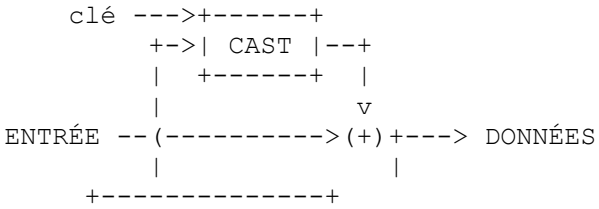
Si une commande START est envoyée (reçue) avec un id_de_clé différent, la machine de chiffrement (déchiffrement) doit être réinitialisée immédiatement après la fin de la commande START avec la nouvelle clé et le vecteur initial envoyés (reçus) dans la dernière commande CFB64_IV.

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

CAST à rebouclage par le chiffre 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 = CAST(iV, clé)
On = Dn ^ Vn
V(n+1) = CAST(On, clé)

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 16 (5) octets, l'option CAST128_CFB64 (CAST5_40_CFB64) ne doit pas être offerte ou utilisée comme option de chiffrement Telnet valide.

Si il y a moins de 32 (10) octets de données de clé, les 16 (5) premiers octets de données de clé sont utilisés comme id_de_clé 0 dans chaque direction. Si il y a au moins 32 (10) octets de données de clé, les 16 (5) premiers octets de données de clé sont utilisés pour chiffrer les données envoyées par le client Telnet au serveur Telnet ; les 16 (5) octets suivants des données de clé sont utilisés pour chiffrer les données envoyées par le serveur Telnet au client Telnet.

Toutes les données de clé supplémentaires sont utilisées comme données aléatoires à envoyer comme vecteur d'initialisation.

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).

Les modes de chiffrement qui utilisent des clés de 40 bits ne sont pas considéré comme sûrs. Le mode de clé à 40 bits CAST5_40_CFB64 n'est cité ici que pour documenter les mises en œuvre qui sont déjà présentes sur l'Internet mais n'avaient jamais été documentées.

7. Remerciements

Le présent document se fonde sur le documence "Chiffrement Telnet : DES à rebouclage de sortie à 64 bits" rédigé à l'origine par Dave Borman de Cray Research avec le concours du groupe de travail Telnet de l'IETF.

8. Références

[RFC2144] C. Adams, "L'algorithme de chiffrement CAST-128", mai 1997. *(Information)*

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.