Groupe de travail Réseau
Request for Comments : 2946
Catégorie : En cours de normalisation

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

Option Telnet de chiffrement des données

Résumé
Le présent document décrit une option de chiffrement Telnet comme méthode générique pour fournir des services de confidentialité des données pour le flux de données Telnet. Bien que le présent document résume les types et codes de chiffrement actuellement utilisés, il ne définit pas un algorithme de chiffrement spécifique. Des documents distincts seront publiés pour définir les mises en œuvre de cette option pour chaque algorithme de chiffrement.

1. Noms et codes des commandes

ENCRYPT : 38

Commandes de chiffrement

IS	0
SUPPORT	1
REPLY	2
START	3
END	4
REQUEST-START	5
REQUEST-END	6
ENC_KEYID	7
DEC_KEYID	8

Types de chiffrement

NULL	0
DES_CFB64	1
DES_OFB64	2
DES3_CFB64	3
DES3_OFB64	4
CAST5_40_CFB64	8
CAST5_40_OFB64	9
CAST128_CFB64	10
CAST128_OFB64	11

Suivant des pratiques historiques, les numéros de type de chiffrement futurs seront alloués par l'IANA selon la politique du premier arrivé premier servi décrite dans la [RFC2434]. En dépit du fait que les numéros de type d'authentification sont alloués dans un espace de numéros de 8 bits (comme le sont la plupart des valeurs dans la spécification Telnet) on ne prévoit pas que cet espace numérique soit en danger d'épuisement ou le devienne ; cependant, si cela devait devenir un problème, lorsque plus de 50 % de l'espace de nombres sera alloué, l'IANA devra adresser les demandes d'allocation à l'IESG ou à un expert désigné pour approbation.

2. Signification des commandes

IAC WILL ENCRYPT
L'envoyeur de cette commande veut envoyer des données chiffrées.

IAC WONT ENCRYPT
L'envoyeur de cette commande refuse d'envoyer des données chiffrées.

IAC DO ENCRYPT
L'envoyeur de cette commande veut recevoir des données chiffrées.

IAC DONT ENCRYPT
L'envoyeur de cette commande refuse d'accepter des données chiffrées.

IAC SB ENCRYPT SUPPORT liste_des_types_de_chiffrement IAC SE
L'envoyeur de cette commande déclare les types de chiffrement qu'il accepte. Seul le côté de la connexion qui est DO ENCRYPT peut envoyer la commande SUPPORT. Les types de chiffrement courants sont énumérés dans la version actuelle du document Numéros alloués [*www.iana.org*].

La liste des types de chiffrement ne peut inclure que des types qui peuvent réellement être pris en charge durant la session en cours. Si ENCRYPT est négocié en conjonction avec AUTH, le message SUPPORT NE DOIT PAS être envoyé tant que la clé de session n'a pas été déterminée. Autrement, il est impossible de savoir si le type de chiffrement choisi peut être correctement initialisé sur la base du type et de la longueur de la clé qui est disponible.

IAC SB ENCRYPT IS type de chiffrement ... IAC SE
L'envoyeur de cette commande déclare le type de chiffrement à utiliser, et toutes les données initiales qui sont nécessaires. Seul le côté de la connexion qui est WILL ENCRYPT peut envoyer la commande IS pour initialiser le schéma de type de chiffrement.

IAC SB ENCRYPT REPLY type de chiffrement ... IAC SE
L'envoyeur de cette commande continue l'échange de données initial afin d'initialiser le schéma de type de chiffrement. Seul le côté de la connexion qui est DO ENCRYPT peut envoyer la commande REPLY.

IAC SB ENCRYPT START id_de_clé IAC SE
L'envoyeur de cette commande déclare que toutes les données qui suivent la commande dans le flux de données seront chiffrées via la méthode précédemment négociée de chiffrement de données. Seul le côté de la connexion qui est WILL ENCRYPT peut envoyer la commande START.

Le id_de_clé est un champ de longueur variable. Il est utilisé par divers mécanismes de chiffrement pour identifier quelle clé de chiffrement sera utilisée, lorsque plusieurs clés de chiffrement peuvent être connues de part et d'autre de la connexion. Le champ id_de_clé est codé avec l'octet de poids fort en premier, et une valeur de id_de_clé de zéro est réservée pour indiquer la clé de chiffrement par défaut (cela sera normalement une clé de chiffrement déduite durant l'authentification, avec l'option AUTHENTICATION). Le champ id_de_clé doit être au moins long d'un octet. Les seules valeurs valides pour "id_de_clé" seront celles qui ont été reçues dans une commande DEC_KEYID.

IAC SB ENCRYPT END IAC SE
L'envoyeur de cette commande déclare que toutes les données qui suivent la commande dans le flux de données seront non chiffrées. Seul le côté de la connexion qui est WILL ENCRYPT peut envoyer le END

IAC SB ENCRYPT REQUEST-START id_de_clé IAC SE
L'envoyeur de cette commande demande que le côté distant commence le chiffrement du flux de données Telnet. Seul le côté de la connexion qui est DO ENCRYPT peut envoyer la commande REQUEST-START. Le id_de_clé est seulement facultatif, et peut être omis.

IAC SB ENCRYPT REQUEST-END IAC SE
L'envoyeur de cette commande demande que le côté distant cesse le chiffrement du flux de données Telnet. Seul le côté de la connexion qui est DO ENCRYPT peut envoyer la commande REQUEST-END.

IAC SB ENCRYPT ENC_KEYID id_de_clé IAC SE
L'envoyeur de cette commande demande que le côté distant vérifie que "id_de_clé" se transpose en une clé valide; ou vérifie que le "id_de_clé" reçu dans une commande DEC_KEYID est valide. Si le id_de_clé est omis, cela implique qu'il n'y a plus de id_de_clé connu, et que la tentative de trouver un id_de_clé commun a échoué. Seul le côté de la connexion

qui est WILL ENCRYPT peut envoyer la commande ENC_KEYID.

IAC SB ENCRYPT DEC_KEYID id_de_clé IAC SE
L'envoyeur de cette commande demande que le côté distant vérifie que le "id_de_clé" se transpose en une clé valide sur le côté distant ; ou vérifie que le "id_de_clé" reçu dans une commande ENC_KEYID est valide. Si le id_de_clé est omis, cela implique qu'il n'y a plus de id_de_clé connu, et que la tentative de trouver un id_de_clé commun a échoué. Seul le côté de la connexion qui est DO ENCRYPT peut envoyer la commande DEC_KEYID.

3. Spécification par défaut

La spécification par défaut pour cette option est

WONT ENCRYPT
DONT ENCRYPT

ce qui signifie qu'il n'y aura aucun chiffrement du flux de données Telnet.

4. Motivation

Le protocole Telnet n'a aucune forme de protection contre l'intervention de passerelles qui surveillent les paquets IP qui voyagent à travers le réseau. C'est particulièrement dangereux lorsque des mots de passe sont envoyés en clair sur le réseau. La présente option donne une méthode pour chiffrer les flux de données.

5. Règles de mise en œuvre

Une fois que l'option Chiffrement est activée, toutes les données dans la direction négociée, y compris les options Telnet, sont chiffrées. Le chiffrement commence avec l'octet de données qui suit immédiatement la commande "IAC SB ENCRYPT START type_de_chiffrement IAC SE". Le chiffrement se termine après la commande "IAC SB ENCRYPT END IAC SE".

WILL et DO ne sont utilisés qu'au début de la connexion pour obtenir et accorder la permission de négociations futures. L'option ENCRYPT doit être négociée dans les deux directions.

Une fois que les deux hôtes ont échangé un WILL et un DO, l'envoyeur du DO ENCRYPT doit envoyer une commande ENCRYPT SUPPORT pour faire savoir au côté distant les types de chiffrement qu'il accepte. Dans la demande, une liste de schémas de chiffrement pris en charge est envoyée. Seul l'envoyeur du DO peut envoyer une liste des types de chiffrement pris en charge (IAC SB ENCRYPT SUPPORT liste_des_types_de_chiffrement IAC SE). Seul l'envoyeur du WILL peut en fait transmettre les données chiffrées. Ceci est initié via la commande "IAC SB ENCRYPT START IAC SE" et terminé via la commande "IAC SB ENCRYPT END IAC SE". Si un START est reçu, et si un second START est reçu avant de recevoir un END, le second START est ignoré.

Si l'envoyeur du DO voulait que le côté distant commence d'envoyer des données chiffrées, il peut envoyer la commande "IAC SB ENCRYPT REQUEST-START IAC SE". Si l'envoyeur du DO voulait que le côté distant cesse d'envoyer des données chiffrées, il peut envoyer la commande "IAC SB ENCRYPT REQUEST-STOP IAC SE".

Si le receveur de la commande SUPPORT ne prend en charge aucun des types de chiffrement énumérés dans la commande SUPPORT, il devrait envoyer une "IAC SB ENCRYPT IS NULL IAC SE" pour indiquer qu'ils n'ont aucun type de chiffrement en commun. Il peut aussi envoyer une commande IAC WONT ENCRYPT pour désactiver l'option ENCRYPT.

L'ordre des types de chiffrement dans une commande SUPPORT doit indiquer une préférence pour les différents types de chiffrement, le premier type étant le préféré, et le dernier type étant le moins préféré.

Si l'option ENCRYPT a été activée, et si des données chiffrées sont reçues, la réception d'un "IAC WONT ENCRYPT" implique la réception d'un "IAC SB ENCRYPT END IAC SE", par exemple, le flux des données Telnet n'est plus chiffré.

L'exemple suivant montre l'utilisation de cette option :

Hôte1 **Hôte2**

[L'Hôte1 demande à l'Hôte2 de négocier le chiffrement des données que l'Hôte2 envoie à l'Hôte1. L'Hôte2 accepte de négocier le chiffrement des données qu'il envoie à l'Hôte1.]

DO ENCRYPT

WILL ENCRYPT

[Hôte1 demande que Hôte2 active le chiffrement aussitôt que l'initialisation est achevée, et informe Hôte2 qu'il prend en charge DES_CFB64.]IAC SB ENCRYPT REQUEST-START IAC SE

IAC SB ENCRYPT SUPPORT DES_CFB64 IAC SE

[Hôte2 envoie le vecteur initial à l'Hôte1. Hôte1 accuse réception du vecteur d'initialisation (IV).]

IAC SB ENCRYPT IS DES_CFB64 CFB64_IV 144 146 63 229 237 148 81 143 IAC SE IAC SB ENCRYPT REPLY DES_CFB64 CFB64_IV_OK 103 207 181 71 224 55 229 98 IAC SE

[L'Hôte2 est maintenant libre de commencer l'envoi des données chiffrées, et comme un REQUEST-START a été reçu, il active le chiffrement.]

IAC SB ENCRYPT START IAC SE

[Toutes les données de l'Hôte2 à l'Hôte1 sont maintenant chiffrées.]

IAC SB ENCRYPT END IAC SE

[Toutes les données de l'Hôte2 à l'Hôte1 sont maintenant à nouveau en clair.]

On s'attend à ce que toute mise en œuvre qui prend en charge l'option Telnet ENCRYPT prenne en charge la totalité de la présente spécification.

6. Considérations pour la sécurité

L'option ENCRYPT utilisée isolément fournit une protection contre les attaques passives mais pas contre les attaques actives. En d'autres termes, elle va protéger contre quelqu'un qui se contente d'observer les paquets IP lorsqu'ils passent à travers le réseau. Cependant, un attaquant qui est capable de modifier les paquets au vol pourrait empêcher l'option ENCRYPT d'être négociée.

On peut remédier à cette faute en utilisant l'option Telnet AUTHENTICATION avec l'option ENCRYPT. Précisément, le réglage ENCRYPT_USING_TELOPT dans la paire_de_type_d'authentification peut être utilisé pour forcer que le chiffrement soit négocié même en face d'attaques actives.

De plus, un attaquant actif peut interférer avec des tentatives de commencer ou recommencer le chiffrement. Si le chiffrement est demandé par l'utilisateur, et si le client n'est pas capable de négocier l'activation ou la réactivation du chiffrement, le client doit supposer qu'il subit une attaque, et il DOIT immédiatement mettre un terme à la connexion Telnet.

7. Directions futures pour le chiffrement Telnet

La spécification définit une méthode pour fournir la confidentialité des données au flux de données Telnet. Malheureusement le mécanisme de chiffrement fourni sous cette option n'assure pas l'intégrité des données, à cause de la complexité de la spécification d'un protocole qui fournisse efficacement des services d'intégrité dans un protocole en mode flux.

La spécification TELNET START_TLS fournit un schéma qui assure la confidentialité, l'intégrité, et la compression, et des travaux futurs sur le chiffrement Telnet devront examiner de près l'utilisation de la présente spécification. Une approche prometteuse utiliserait le mode Diffie-Hellman anonyme de TLS, suivi par l'option Telnet AUTHENTICATION où le mécanisme d'authentification inclurait les messages terminés de client et serveur calculés durant la négociation TLS.

8. Remerciements

Le présent document a été à l'origine écrit par Dave Borman de Cray Research, avec l'assistance de Theodore Ts'o du MIT et du groupe de travail Telnet de l'IETF.

9. Références

[RFC0854] J. Postel et J. Reynolds," Spécification du protocole Telnet", STD 8, mai 1983.

[RFC2941] T. Ts'o, éd., J. Altman, "Option d'authentification Telnet", septembre 2000. *(P.S.)*

[RFC2434] T. Narten et H. Alvestrand, "Lignes directrices pour la rédaction d'une section Considérations relatives à l'IANA dans les RFC", BCP 26, octobre, 1998. *(Rendue obsolète par la RFC 5226)*

10. Adresse de l'auteur

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

11. Déclaration complète de droits de reproduction

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