Groupe de travail Réseau
Request for Comments : 2419
RFC rendue obsolète : 1969
Catégorie : En cours de normalisation

K. Sklower, University of California, Berkeley
G. Meyer, Shiva
septembre 1998
Traduction Claude Brière de L'Isle

Protocole de chiffrement DES pour PPP, version 2 (DESE-bis)

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

Résumé
Le protocole point à point (PPP) [RFC1661] donne une méthode standard pour transporter des datagrammes multi protocoles sur des liaisons point à point. Le protocole de contrôle de chiffrement (ECP, *Encryption Control Protocol*) sur PPP [RFC1968] donne une méthode pour négocier et utiliser les protocoles de chiffrement sur des liaisons encapsulées en PPP.
Le présent document donne les détails spécifiques pour l'utilisation de la norme DES [FIPS-46], [FIPS-81], pour chiffrer des paquets encapsulés en PPP.

Remerciements
Les auteurs remercient chaleureusement Fred Baker de Cisco, Philip Rakity de Flowpoint, et William Simpson de Daydreamer des améliorations qu'ils ont apportées à la clarté et la justesse de ce document.

Table des Matières

1. Introduction

1.1 Motivation

L'objet du présent mémoire est double : montrer comment on spécifie les nécessaires détails d'un protocole de "données" ou de "support" dans le contexte d'un protocole générique de contrôle de chiffrement pour PPP, et aussi fournir au moins un moyen compris généralement pour sécuriser la transmission de données entre les mises en œuvre de PPP.

L'algorithme de chiffrement DES a été bien étudié, compris et largement mis en œuvre. Le chiffrement DES a été conçu pour une mise en œuvre efficace dans les matériels, et peut par conséquent être relativement coûteux à mettre en œuvre dans les logiciels. Cependant, son omniprésence en fait un choix raisonnable comme protocole de chiffrement "modèle".

Le code source qui met en œuvre DES dans le "mode de livre de code électronique" se trouve dans [SCHNEIER]. Les lois des USA sur l'exportation interdisent l'inclusion de code source prêt à la compilation dans le présent document.

1.2 Conventions

Les mots clés "DOIT", "NE DOIT PAS", "EXIGE", "DEVRA", "NE DEVRA PAS", "DEVRAIT", "NE DEVRAIT PAS", "PEUT", et "FACULTATIF" dans le présent document sont à interpréter comme décrit dans la [RFC2119].

2. Généralités

L'objet du chiffrement des paquets échangés entre deux mises en œuvre de PPP est de tenter de s'assurer de la confidentialité de la communication effectuée via les deux mises en œuvre. Le processus de chiffrement dépend de la spécification d'un algorithme de chiffrement et d'un secret partagé (impliquant usuellement au moins une clé) entre l'envoyeur et le receveur.

Généralement, le chiffreur va prendre un paquet PPP incluant le champ Protocole, va appliquer l'algorithme de chiffrement choisi, placer le texte chiffré résultant (et dans la présente spécification, un numéro de séquence explicite) dans le champ Information d'un autre paquet PPP. Le déchiffreur va appliquer l'algorithme inverse et interpréter le texte en clair résultant comme si c'était un paquet PPP qui était arrivé directement sur l'interface.

Les moyens par lesquels le secret est porté à la connaissance des deux éléments communicants sort du domaine d'application du présent document ; une certaine forme de configuration manuelle est généralement impliquée. Les mises en œuvre peuvent faire usage de l'authentification PPP, ou de l'option Identifiant de point d'extrémité décrite dans PPP multi liaison [RFC1990], comme facteurs de choix du secret partagé. Si le secret peut être déduit par l'analyse de la communication entre les deux parties, aucune confidentialité n'est alors garantie.

Bien que l'algorithme de la norme de chiffrement des données (DES, *Data Encryption Standard*) des USA [FIPS-46], [FIPS-81] fournisse plusieurs modes d'utilisation, la présente spécification choisit l'utilisation d'un seul mode conjointement avec le protocole de contrôle de chiffrement (ECP, *Encryption Control Protocol*) de PPP : le mode de chaînage de bloc de chiffrement (CBC, *Cipher Block Chaining*). En plus des publications du gouvernement des USA citées ci-dessus, le mode CBC est aussi exposé dans [SCHNEIER], bien qu'aucun code source en langage C ne soit fourni pour lui.

Le vecteur d'initialisation pour ce mode est déduit d'un nom occasionnel explicite de 64 bits, qui est échangé en clair durant la phase de négociation. La clé de 56 bits exigée par tous les modes DES est établie comme secret partagé entre les mises en œuvre.

Une raison du choix du mode de chaînage est qu'on pense généralement qu'il exige plus de ressources de calcul pour déduire une clé de 64 bits pour le chiffrement DES par l'analyse du flux de communication chiffrée lorsque le mode de chaînage est utilisé, par rapport à la situation où chaque bloc est chiffré séparément sans chaînage. Il est certain que des séquences identiques de texte en clair vont produire des chiffrements différents lorsque le mode chaînage est en effet, compliquant ainsi l'analyse.

Cependant, si le chaînage doit s'étendre au delà des limites d'un paquet, l'envoyeur et le receveur doivent tous deux s'entendre sur l'ordre dans lequel les paquets ont été chiffrés. Donc, la présente spécification fournit un numéro de séquence explicite de 16 bits pour décrire la séquence de déchiffrement des paquets. Ce mode de fonctionnement permet même la récupération de pertes occasionnelles de paquets ; les détails sont aussi donnés plus loin.

3. Structure de la spécification

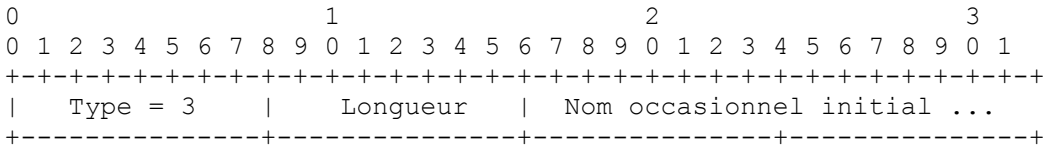
Le protocole de contrôle de chiffrement PPP (ECP), fournit un cadre pour la négociation des paramètres associés au chiffrement, tels que le choix de l'algorithme. Il spécifie les numéros alloués à utiliser comme numéros de protocole PPP pour les "paquets de données" à transporter comme "protocole de données" associé, et décrit l'automate à états.

Donc, une spécification à utiliser dans cette matrice a seulement besoin de décrire les options de configuration supplémentaires requises pour spécifier un algorithme particulier, et le processus par lequel on chiffre/déchiffre les informations une fois que l'état Ouvert a été atteint.

4. Option de configuration DESE pour ECP

Description
L'option de configuration DESE d'ECP indique que la mise en œuvre qui la produit offre d'employer cette spécification pour déchiffrer les communications sur la liaison, et elle peut être vue comme une demande que son homologue chiffre les paquets de cette manière.
L'option de configuration DESE d'ECP a les champs suivants, qui sont transmis de gauche à droite :

Figure 1 : option de configuration DESE d'ECP



Type = 3, pour indique le protocole DESE-bis. L'ancienne valeur de 1 indiquant la précédente spécification DESE est déconseillée, c'est-à-dire que les systèmes qui mettent en œuvre la présente spécification NE DOIVENT PAS offrir l'ancienne valeur 1 dans une demande de configuration et DOIVENT faire un rejet de configuration à réception de l'ancienne valeur d'une demande de configuration qui la contient.

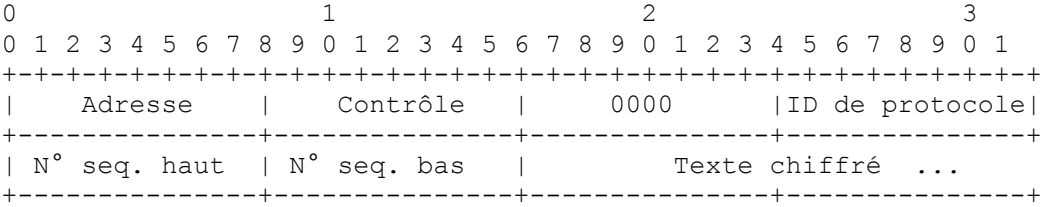
Longueur : 10

Nom occasionnel initial
Ce champ est une quantité de 8 octets qui est utilisée par la mise en œuvre homologue pour chiffrer le premier paquet transmis après que l'envoyeur a atteint l'état Ouvert.
Pour se prémunir contre les attaques en répétition, la mise en œuvre DEVRAIT offrir une valeur différente durant chaque négociation ECP. Un exemple pourrait être d'utiliser le nombre de secondes depuis le premier janvier 1970 (GMT/UT) dans les 32 bits premiers bits, et le nombre actuel de nanosecondes par rapport à la dernière marque de seconde dans les 32 derniers bits.
Son rôle dans la formulation est décrit dans la section Chiffrement ci-dessous.

5. Format de paquet pour DESE

Description
Les paquets DESE ont eux-mêmes les champs suivants :

Figure 2 : Format de paquet de protocole de chiffrement DES



Adresse et Contrôle
Ces champs DOIVENT être présents sauf si l'option de compression des champs Adresse et Contrôle PPP (ACFC, *Address and Control Field Compression*) a été négociée.

ID de protocole
La valeur de ce champ est 0x53 ou 0x55 ; cette dernière indique que le texte chiffré inclut des en-têtes pour le protocole multi liaison , et EXIGE que le protocole de contrôle de chiffrement de liaison individuelle ait atteint l'état Ouvert. Le zéro en tête PEUT être absent si l'option Compression de champ de protocole PPP (PPC, *Protocol Field Compression*) a été négociée.

Numéro de séquence
Ces nombres de 16 bits sont alloués en séquence par le chiffreur en commençant par 0 (pour le premier paquet transmis une fois que ECP a atteint l'état Ouvert.

Texte chiffré
La génération de ces données est décrite dans la section suivante.

6. Chiffrement

Une fois que ECP a atteint l'état Ouvert, l'envoyeur NE DOIT PAS appliquer la procédure de chiffrement aux paquets LCP ni aux paquets ECP.

Si l'option Transposition de caractère de contrôle asynchrone a été négociée sur la liaison, l'envoyeur applique la transposition après le fonctionnement de l'algorithme de chiffrement.

L'algorithme de chiffrement est généralement de bourrer les champs Protocole et Information d'un paquet PPP pour l'aligner sur un multiple de 8 octets, et d'applique DES en mode de chiffrement à chaînage de bloc avec une clé K de 56 bits.

Il y a un grand nombre de détails concernant ce qui constitue les champs Protocole et Information, en présence ou non présence de multi liaison, et si les options ACFC et PFC ont été négociées, et la sorte de bourrage choisi.

Sans considérer si ACFC a été négocié sur la liaison, l'envoyeur applique la procédure de chiffrement à la seule portion du paquet qui exclut le champ Adresse et Contrôle.

Si le protocole multi liaison a été négocié et si le chiffrement doit être construit comme étant appliqué séparément à chaque liaison, la procédure de chiffrement est à appliquer aux champs (éventuellement étendus) Protocole et Information du paquet dans le protocole multi liaison.

Si le protocole multi liaison a été négocié et si le chiffrement a été construit comme étant appliqué au faisceau, la procédure multi liaison est alors à appliquer aux paquets DESE résultants.

6.1 Considérations de bourrage

Comme l'algorithme DES fonctionne sur des blocs de 8 octets, les paquets de texte en clair dont la longueur n'est pas un multiple de 8 octets doivent subir un bourrage. Cela peut nuire à l'interprétation de certains protocoles qui ne contiennent pas un champ de longueur explicite dans leurs en-têtes de protocole.

Comme il n'y a pas de répertoire standard des protocoles qui sont susceptibles de corruption par suite du bourrage, cela peut conduire à une certaine confusion quant aux protocoles qui devraient être protégés contre la corruption induite par les bourrages. Par conséquent, la présente spécification exige que la technique non ambiguë décrite ci-dessous soit appliquée à TOUS les paquets de texte en clair.

La méthode du bourrage se fonde sur celle décrite pour l'option de bourrage auto descriptif (SDP, *Self-Describing-Padding*) de LCP (comme définie dans la [RFC1570]), mais diffère sous deux aspects : d'abord, la valeur maximum du bourrage est fixée à 8, et ensuite, la méthode est à appliquer à TOUS les paquets, pas seulement aux "protocoles spécifiquement identifiés".

Le texte en clair qui n'est pas un multiple de 8 octets DOIT être bourré avant le chiffrement du texte en clair avec suffisamment d'octets dans la séquence des octets 1, 2, 3 ... 7 pour faire du texte en clair un multiple de 8 octets.

Le texte en clair qui est déjà un multiple de 8 octets peut exiger un bourrage avec encore 8 octets (1, 2, 3 ... 8). Ces octets supplémentaires DOIVENT être ajoutés avant le chiffrement du texte en clair si le dernier octet du texte a une valeur de 1 à 8, inclus.

Après que l'homologue a déchiffré le texte chiffré, il supprime les octets du bourrage auto descriptif, pour recréer le texte en clair d'origine.

Noter qu'après le déchiffrement, seul le contenu du dernier octet a besoin d'être examiné pour déterminer combien d'octets de bourrage devraient être retirés. Cependant, l'homologue DEVRAIT éliminer la trame si tous les octets qui forment le

bourrage ne correspondent pas au schéma qui vient d'être décrit.

L'opération de bourrage décrite ci-dessus est effectuée indépendamment du fait que l'option de bourrage auto descriptif (SDP) de LCP a été ou non négociée. Si elle l'a été, SDP sera appliqué au paquet comme un tout après qu'il a été chiffré et après qu'a été ajouté l'identifiant de protocole de chiffrement.

6.2 Génération du texte chiffré

Dans cet exposé, E[k] note le chiffrement DES de base déterminé par une clé de 56 bits k agissant sur des blocs de 64 bits. et D[k] note le mécanisme de déchiffrement correspondant. Le texte en clair bourré décrit au paragraphe précédent devient alors une séquence de blocs de 64 bits P[i] (ou i est dans la gamme de 1 à n). Le caractère accent circonflexe (^) représente l'opération de OU exclusif au bit près appliquée aux blocs de 64 bits.

Lors du chiffrement du premier paquet à transmettre dans l'état Ouvert, soit C[0] le résultat de l'application de E[k] au nom occasionnel initial reçu dans l'option DESE ECP de l'homologue ; autrement, soit C[0] le bloc final du paquet transmis précédemment.

Le texte chiffré pour le paquet est généré par le processus itératif C[i] = E[k](P[i] ^ C[i-1]) pour i variant de 1 à n.

6.3 Restitution du texte en clair

Lors du déchiffrement du premier paquet reçu dans l'état Ouvert, soit C[0] le résultat de l'application de E[k] au nom occasionnel initial transmis dans l'option DESE d'ECP. Le premier paquet aura le numéro de séquence zéro. Pour les paquets suivants, soit C[0] le bloc final du paquet précédent dans l'espace des numéros de séquence. Le déchiffrement est alors accompli par : P[i] = C[i-1] ^ D[k](C[i]), pour i entre 1 et n.

6.4 Récupération de perte de paquet

La perte de paquet est détectée lorsque il y a une discontinuité dans les numéros de séquence des paquets consécutifs. Supposons que le paquet de numéro N - 1 a une erreur irrécupérable ou est perdu, mais que les paquets N et N + 1 sont reçus correctement.

Comme l'algorithme de la section précédente exige que C[0] pour le paquet N soit C[der] pour le paquet N - 1, il sera impossible de décoder le paquet N. Cependant, tous les paquets N + 1 et les suivants peuvent être décodés de la façon habituelle, car tout ce qui est exigé est le dernier bloc de texte chiffré du paquet précédent (dans ce cas, le paquet N, qui a été reçu).

7. Considérations de MRU

Comme le bourrage peut intervenir, et parce qu'il y a un champ Protocole supplémentaire qui agit, les mises en œuvre devraient prendre en compte la croissance des paquets. Par exemple, si PFC avait été négocié, et si la MRU avait été précédemment exactement un multiple de 8, alors le texte en clair résultant en combinant des paquets de données de pleine taille avec un champ de protocole d'un octet exigerait sept octets supplémentaires de bourrage, et le numéro de séquence ferait deux octets supplémentaires de sorte que le champ Information dans le protocole DESE ferait maintenant 10 octets de plus que dans le paquet d'origine. Comme la convention est que les options PPP sont indépendantes les unes des autres, la négociation de DESE n'augmente pas automatiquement, par elle-même, la valeur de la MRU.

8. Différences avec la RFC1969

8.1 Quand effectuer le bourrage

Dans la RFC1969, la méthode de bourrage auto descriptif n'était pas appliquée à tous les paquets transmis en utilisant DESE. Suivant la méthode de l'option SDP elle-même, seuls les "protocoles spécifiquement identifiés" étaient à bourrer. Les protocoles avec un identifiant de longueur explicite en étaient exempts. (Les exemples incluent VJ IP non compressé, XNS, CLNP).

Dans la présente spécification, la méthode est appliquée à TOUS les paquets.

Ensuite, il a été précisé dans cette spécification qu'elle est complètement indépendante de l'option de bourrage auto

descriptif pour PPP, et elle fixe le nombre maximum d'octets de bourrage à 8.

8.2 Numéros alloués

Comme la présente spécification pourrait théoriquement causer une mauvaise interprétation d'un paquet transmis conformément à la spécification précédente, un nouveau numéro de champ de type a été alloué pour le protocole DESE-bis.

8.3 Changements rédactionnels mineurs

Cette spécification a été conçue comme un document en cours de normalisation. Certaines expressions ont été changées pour être plus clair.

9. Considérations pour la sécurité

Cette proposition s'attache a fournir seulement la confidentialité. Elle ne décrit aucun mécanisme pour l'intégrité, l'authentification ou la non répudiation. Elle ne garantit pas qu'un message reçu n'a pas été modifié dans le transit par une répétition, coupé-collé ou une altération active. Elle n'assure pas l'authentification de la source d'un paquet reçu, ni ne protège contre la possibilité que l'envoyeur d'un message nie en être l'auteur.

Cette proposition s'appuie sur des méthodes extérieures et non spécifiées pour l'authentification et la restitution des secrets partagés. Elle ne propose pas de nouvelle technologie pour la confidentialité, mais décrit simplement une convention pour l'application du chiffrement DES aux transmissions de données entre des mises en œuvre de PPP.

Toutes les méthodologies pour la protection et la restitution des secrets partagés, et toutes les limitations du chiffrement DES sont pertinentes pour l'utilisation décrite ici.

10. Références

[FIPS-46] National Bureau of Standards, "Data Encryption Standard", FIPS PUB 46 (janvier 1977).

[FIPS-81] Ntional Bureau of Standards, "DES Modes of Operation", FIPS PUB 81 (décembre 1980).

[RFC1570] W. Simpson, "Extensions LCP pour PPP", janvier 1994. *(P.S., MàJ par* RFC2484*)*

[RFC1661] W. Simpson, éditeur, "Protocole point à point (PPP)", STD 51, juillet 1994. *(MàJ par la* RFC2153)

[RFC1968] G. Meyer, "Protocole de contrôle de chiffrement en PPP (ECP)", juin 1996. *(P.S.)*

[RFC1990] K. Sklower et autres, "Protocole multiliaison en PPP (MP)", août 1996. (*Remplace* RFC1717) *(D.S.)*

[RFC2119] S. Bradner, "Mots clés à utiliser dans les RFC pour indiquer les niveaux d'exigence", BCP 14, mars 1997.

[SCHNEIER] Schneier, B., "Applied Cryptography - Protocols Algorithms, and source code in C", John Wiley & Sons, Inc. 1994. Un errata est associé à ce livre, et on peut en avoir copie en envoyant un message à schneier@counterpane.com

11. Adresse des auteurs

Keith Sklower
Computer Science Department
339 Soda Hall, Mail Stop 1776
University of California
Berkeley, CA 94720-1776
téléphone : (510) 642-9587
mél : sklower@CS.Berkeley.EDU

Gerry M. Meyer
Cisco Systems Ltd.
Bothwell House, Pochard Way,
Strathclyde Business Park,
Bellshill, ML4 3HB
Scotland, UK
mél : gemeyer@cisco.com

12. Déclaration complète de droits de reproduction