Groupe de travail Réseau
Request for Comments : 2406
Rendue obsolète : 1827
Catégorie : Norme
Novembre 1998

S. Kent, BBN Corp
R. Atkinson, @Home Network

Traduction Claude Brière de L'Isle

Incorporation de charge utile de sécurité sur IP (ESP)

Statut du présent Mémo

Le présent document spécifie un protocole normalisé de l'Internet pour la communauté de l'Internet, et appelle à discussion et suggestions pour son amélioration. Prière de se reporter à l'édition en cours des normes officielles du protocole Internet "Internet Official Protocol Standards" (STD 1) pour l'état de la normalisation et le statut du présent protocole. La distribution du présent mémo n'est soumise à aucune restriction.

Déclaration de copyright

Table des matières

1 Introduction

L'en-tête d'incorporation de charge utile de sécurité (ESP, *Encapsulating Security Payload*) est destiné à fournir une combinaison des services de sécurité dans IPv4 et IPv6. ESP peut s'appliquer seul, en combinaison avec l'en-tête d'authentification IP [KA97b], ou de façon incorporée, par exemple, en utilisant un mode tunnel (voir "Architecture de sécurité pour le protocole Internet" [KA97a], auquel on se réfère ci-après comme document Architecture de sécurité). Les services de sécurité peuvent être fournis entre une paire d'hôtes communicants, entre une paire de passerelles de sécurité communicantes, ou entre une passerelle de sécurité et un hôte. Pour des précisions sur la façon d'utiliser ESP et en-tête d'authentification dans divers environnements de réseau, voir le document Architecture de sécurité [KA97a].

L'en-tête ESP est inséré après l'en-tête IP et avant l'en-tête de protocole de couche supérieure (mode transport) ou avant un en-tête IP incorporé (mode tunnel). Ces modes sont décrits plus en détail ci-dessous.

ESP sert à fournir la confidentialité, l'authentification de l'origine des données, l'intégrité sans connexion, un service anti-répétition (forme d'intégrité de séquence partielle), et une confidentialité limitée de flux de trafic. L'ensemble des services fournis dépend des options choisies au moment de l'établissement de l'association de sécurité et du placement de la mise en oeuvre. La confidentialité peut être choisie indépendamment de tous les autres services. Cependant, utiliser la confidentialité sans l'intégrité/authentification (dans ESP ou séparément en en-tête d'authentification (AH) peut soumettre le trafic à certaines formes d'attaques actives qui pourraient saper le service de confidentialité (voir [Bel96]). L'authentification d'origine des données et l'intégrité sans connexion sont des services conjoints (auxquels on se réfère conjointement ci-après sous le nom de "authentification) et qui sont offerts comme une option en conjonction avec la confidentialité. Le service anti-répétition ne peut être choisi que si l'authentification d'origine des données est choisie, et ce choix est à la seule discrétion du receveur. (Bien que par défaut, l'envoyeur incrémente le numéro de séquence utilisé pour l'anti-répétition, le service n'est effectif que si le receveur vérifie le numéro de séquence.) La confidentialité des flux de trafic requiert le choix du mode tunnel, et elle est la plus efficace si elle est mise en œuvre à une passerelle de sécurité, où l'agrégation du trafic peut être capable de masquer les vrais schémas de source-destination. Noter que bien que la confidentialité et l'authentification soient toutes deux facultatives, au moins une d'elles DOIT être choisie.

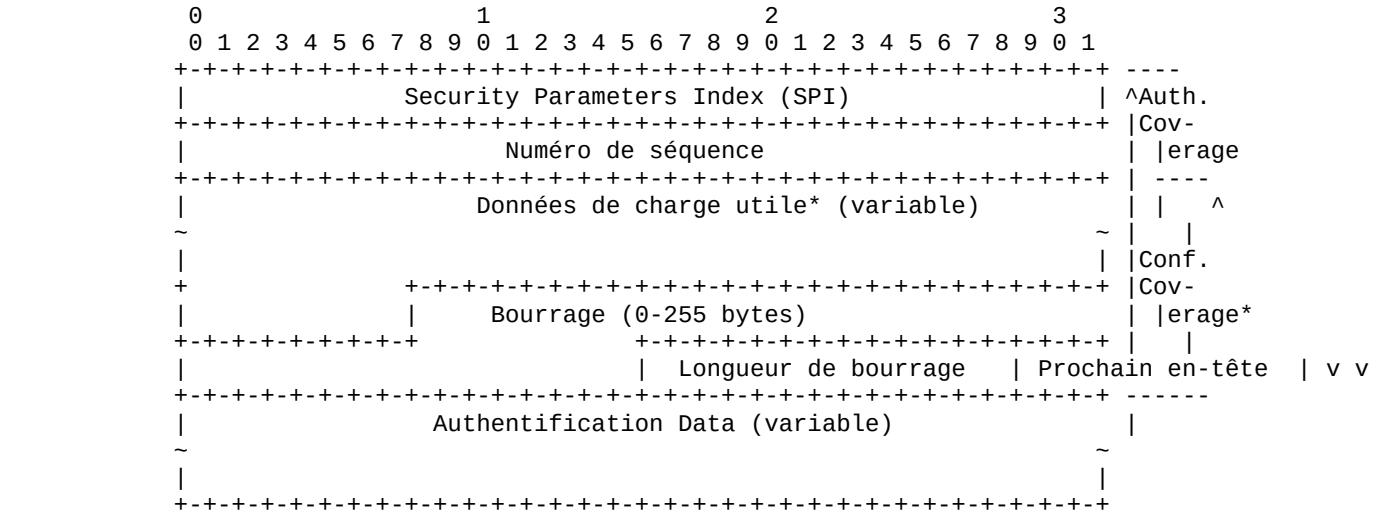
On suppose que le lecteur est familier avec les termes et concepts décrits dans le document Architecture de sécurité. En particulier, le lecteur devrait être familiarisé avec les définitions de services de sécurité offerts par ESP et d'en-tête d'authentification, le concept d'associations

de sécurité, les façons dont ESP peut être utilisé en conjonction avec l'en-tête d'authentification (AH), et les différentes options de gestion de clé disponibles pour ESP et l'en-tête d'authentification. (En ce qui concerne ce dernier sujet, les options courantes de gestion de clé nécessaires à la fois pour l'en-tête d'authentification et ESP sont l'entrée manuelle et l'entrée automatisée via IKE [HC98].)

Les mots clé DOIT, NE DOIT PAS, REQUIS, DEVRAIT, NE DEVRAIT PAS, RECOMMANDÉ, PEUT, et FACULTATIF, lorsque ils apparaissent dans le présent document, sont à interpréter comme décrit dans la RFC 2119 [Bra97].

2 Format de paquet d'incorporation de charge utile de sécurité

L'en-tête de protocole (IPv4, IPv6, ou extension) précédent immédiatement l'en-tête ESP va contenir la value 50 dans son champ d'en-tête de protocole (IPv4) ou suivant (IPv6, extension) [STD-2].



* Si elles sont incluses dans le champ de charge utile, les données de synchronisation cryptographique, par exemple, un vecteur d'initialisation (IV, voir le paragraphe 2.3), ne sont pas habituellement chiffrées par elles-mêmes, bien qu'elles soient souvent considérées comme faisant partie du texte chiffré.

Les paragraphes suivants définissent les champs de format d'en-tête.
"Facultatif" signifie que le champ est omis si l'option n'est pas choisie, c'est-à-dire qu'elle n'est présente ni dans le paquet tel qu'il est transmis ni tel qu'il est formaté pour le calcul d'une valeur de vérification d'intégrité (ICV, *Integrity Check Value*, voir le paragraphe 2.7). Qu'une option soit choisie ou non est défini au titre de l'établissement de l'association de sécurité (SA). Et donc, le format des paquets ESP pour une association de sécurité donnée est fixé, pour la durée de l'association de sécurité. A l'opposé, les champs "obligatoires" sont toujours présents dans le format de paquet ESP, pour toutes les associations de sécurité.

2.1 Indice de paramètres de sécurité

L'indice de paramètre de sécurité (SPI) est une valeur arbitraire de 32 bits qui, combinée avec l'adresse IP de destination et le protocole de sécurité (ESP), identifie de façon univoque l'association de sécurité pour ce datagramme. L'ensemble des valeurs de SPI dans la gamme de 1 à 255 est réservée par l'Autorité d'allocation des numéros Internet (IANA) pour une utilisation future ; une valeur SPI réservée ne sera normalement pas allouée par l'IANA sauf si l'utilisation de la valeur SPI allouée est spécifiée dans une RFC. Le SPI est d'ordinaire choisi par le système de destination lors de l'établissement d'une association de sécurité (pour plus de détails, se reporter au document Architecture de sécurité). Le champ SPI est obligatoire.
La valeur SPI zéro (0) est réservée pou une utilisation locale, spécifique de la mise en œuvre et NE DOIT PAS être envoyée sur le réseau. Par exemple, une mise en œuvre de gestion de clés PEUT utiliser la valeur de SPI de zéro pour signifier "Il n'existe pas d'association de sécurité" durant la période où la mise en œuvre IPsec a demandé que cette entité de gestion de clés établisse une nouvelle association de sécurité, mais que celle-ci n'a pas encore été établie.

2.2 Numéro de séquence

Ce champ de 32 bits non signés contient une valeur de compteur à accroissement monotone (le numéro de séquence). Il est obligatoire et est toujours présent même si le receveur n'a pas choisi d'activer le service anti-répétition pour une association de sécurité spécifique. Le traitement du champ numéro de séquence est à la discrétion du receveur, c'est-à-dire que l'envoyeur DOIT toujours émettre ce champ, mais le receveur n'a pas besoin d'agir sur lui (voir l'exposé sur la vérification de numéro de séquence dans le paragraphe "Traitement du paquet entrant" ci-dessous).

Le compteur de l'envoyeur et le compteur du receveur sont initialisés à 0 lorsqu'une association de sécurité est établie. (Le premier paquet envoyé en utilisant une association de sécurité donnée aura un numéro de séquence de 1 ; voir le paragraphe 3.3.3 pour des précisions sur la façon dont est généré le numéro de séquence.) Si l'anti-répétition est activée (par défaut), le numéro de séquence transmis ne doit jamais effectuer un cycle. Et donc, le compteur de l'envoyeur et le compteur du receveur DOIVENT être remis à zéro (en établissant une nouvelle association de sécurité, et donc une nouvelle clé) avant la transmission du 2^{32}ème paquet sur une association de sécurité.

2.3 Données de charge utile

Données de charge utile est un champ de longueur variable qui contient les données décrites dans le champ d'en-tête suivant. Le champ données de charge utile est obligatoire et sa longueur est un nombre entier d'octets. Si l'algorithme utilisé pour chiffrer la charge utile exige des données de synchronisation de chiffrement, par exemple, un vecteur d'initialisation (IV), ces données PEUVENT alors être portées explicitement dans le champ charge utile. Tout algorithme de chiffrement qui exige de telles données explicites de synchronisation par paquet DOIT indiquer la longueur, toute structure de telles données, et la localisation de ces données au titre d'une RFC spécifiant comment l'algorithme doit s'utiliser avec ESP. Si de telles données de synchronisation sont implicites, l'algorithme pour déduire les données DOIT faire partie de la RFC.

Noter que pour assurer l'alignement du texte chiffré (réel) en présence d'un vecteur d'initialisation :

- Pour certains modes de fonctionnement fondés sur un vecteur d'initialisation, le receveur traite le vecteur d'initialisation comme le début du texte chiffré, en l'introduisant directement dans l'algorithme. Dans ces modes, l'alignement du début du texte chiffré (réel) ne pose pas de problème chez le receveur.
- Dans certains cas, le receveur lit le vecteur d'initialisation séparément du texte chiffré. Dans ces cas, la spécification de l'algorithme DOIT préciser comment l'alignement du texte chiffré (réel) doit se faire.

2.4 Bourrage (pour le chiffrement)

Plusieurs facteurs exigent ou motivent l'utilisation du champ de bourrage.

- Si l'algorithme de chiffrement employé exige que le texte en clair soit un multiple d'un certain nombre d'octets, par exemple, la taille de bloc d'un bloc de chiffrement, le champ de bourrage sert à remplir le texte en clair (qui comporte les champs Données de charge utile, Longueur de bourrage et Prochain en-tête, ainsi que Bourrage) jusqu'à la taille requise par l'algorithme.
- Le bourrage peut aussi être exigé, sans considération des exigences de l'algorithme de chiffrement, pour assurer que le texte chiffré résultant se termine sur une limite de quatre octets. Précisément, les champs Longueur de bourrage et Prochain en-tête doivent être alignés à droite au sein d'un mot de quatre octet, comme illustré dans la figure de format de paquet ESP ci-dessus, pour assurer que le champ de données d'authentification (s'il est présent) est aligné sur une limite de quatre octets.
- On peut utiliser le bourrage au-delà de ce qui est exigé pour l'algorithme ou pour les raisons d'alignement citées ci-dessus, pour cacher la longueur réelle de la charge utile, au service de la confidentialité (partielle) du flux de trafic. Cependant, l'inclusion d'un tel bourrage supplémentaire a des implications négatives sur la bande passante et son utilisation devrait faire l'objet d'une attention particulière.

L'envoyeur PEUT ajouter 0 à 255 octets de bourrage. L'inclusion du champ de bourrage dans un paquet ESP est facultative, mais toutes les mises en œuvre DOIVENT prendre en charge la création et l'utilisation du bourrage.

a. Pour s'assurer que les bits à chiffrer sont un multiple de la taille de bloc de l'algorithme (premier tiret ci-dessus), le calcul du bourrage s'applique aux données de charge utile à l'exclusion des champs Vecteur d'initialisation, Longueur de bourrage et Prochain en-tête.

b. Pour s'assurer que les données d'authentification sont alignées sur une limite de quatre octets (second tiret ci-dessus), le calcul du bourrage s'applique aux données de charge utile y compris les champs Vecteur d'initialisation, Longueur de bourrage, et Prochain en-tête.

Si les octets de bourrage sont nécessaires mais que l'algorithme de chiffrement ne spécifie pas le contenu du bourrage, le traitement par défaut suivant DOIT alors être utilisé. Les octets de bourrage sont initialisés avec une série de valeurs entières (non signées, d'un octet). Le premier octet de bourrage ajouté au texte clair est numéroté 1, et les octets de bourrage suivants forment une séquence à croissance monotone : 1, 2, 3, ... Lorsqu'on utilise ce schéma de bourrage, le receveur DEVRAIT inspecter le champ de bourrage. (Ce schéma a été choisi à cause de sa relative simplicité, de la facilité de mise en œuvre dans les matériels et parce qu'il offre une protection limitée contre certaines formes d'attaques de "couper-coller" en l'absence

d'autres mesures de défense de l'intégrité, si le receveur vérifie les valeurs de bourrage au déchiffrement.)

Tout algorithme de chiffrement qui nécessite un bourrage autre que celui par défaut décrit ci-dessus, DOIT définir le contenu du bourrage (par exemple, des zéros ou des données aléatoires) et tout traitement requis du receveur pour ces octets de bourrage dans une RFC spécifiant comment l'algorithme est utilisé avec ESP. Dans de telles circonstances, le contenu du champ Bourrage sera déterminé par l'algorithme de chiffrement et son mode choisi et défini dans la RFC de l'algorithme correspondant. La RFC de l'algorithme pertinent PEUT spécifier qu'un receveur DOIT inspecter le champ de bourrage ou qu'un receveur DOIT informer les envoyeurs de la façon dont il va traiter le champ de bourrage.

2.5 Longueur de bourrage

Le champ Longueur de bourrage indique le nombre d'octets de bourrage le précédant immédiatement. La gamme des valeurs valides est 0 à 255, où une valeur de zéro indique qu'il n'y a pas d'octet de bourrage. Le champ Longueur de bourrage est obligatoire.

2.6 Prochain en-tête

Le champ Prochain en-tête a huit bits et il identifie le type de données contenues dans le champ Données de charge utile, par exemple, un en-tête d'extension en IPv6 ou un identifiant de protocole de couche supérieure. La valeur de ce champ est choisie dans l'ensemble des numéros de protocole IP définis dans la plus récente RFC des "Numéros alloués" [STD-2] de l'Autorité des numéros Internet alloués (IANA). Le champ Prochain en-tête est obligatoire.

2.7 Données d'authentification

Le champ Données d'authentification a une longueur variable et il contient une valeur de vérification d'intégrité (ICV) calculée sur le paquet ESP moins les données d'authentification. La longueur de ce champ est spécifiée par la fonction d'authentification choisie. Le champ Données d'authentification est facultatif, et il n'est inclus que si le service d'authentification a été choisi pour l'association de sécurité en question. La spécification d'algorithme d'authentification DOIT spécifier la longueur de la valeur de vérification d'intégrité et les règles de comparaison et les étapes du traitement pour la validation.

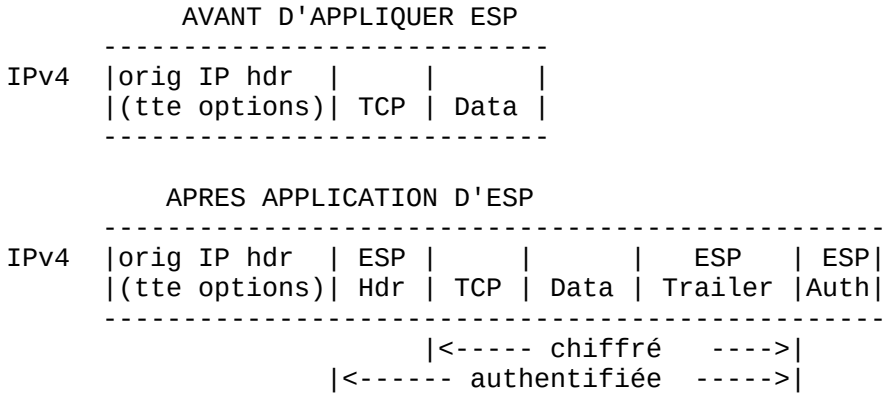
3. Traitement du Protocole d'encapsulation de sécurité

3.1 Localisation de l'en-tête ESP

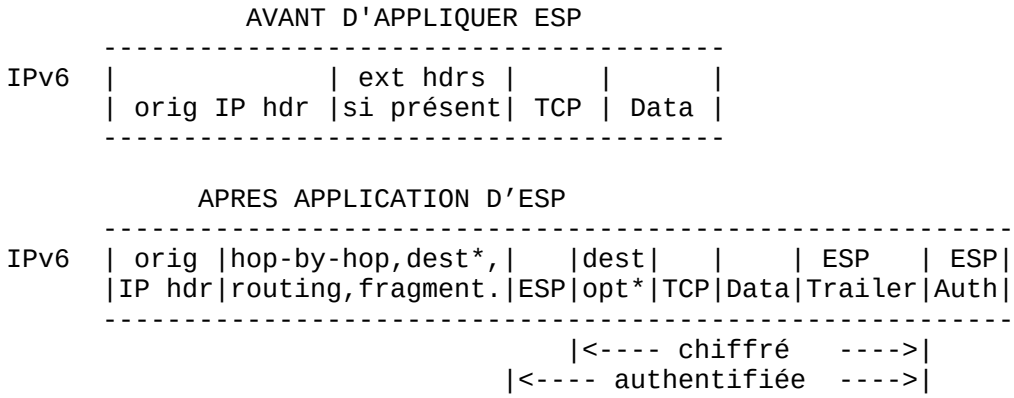
Comme en-tête d'authentification, ESP peut être employé de deux façons : en mode transport ou en mode tunnel. Le premier mode n'est applicable qu'aux mises en œuvre d'hôte et fournit une protection pour les protocoles de couche supérieure, mais pas l'en-tête IP. (Dans ce mode, noter que pour les mises en œuvre "bump-in-the-stack" (*pris dans la pile*) ou "bump-in-the-wire" (*pris sur le réseau*), comme définies dans le document Architecture de sécurité, les

fragments IP entrants ou sortants peuvent exiger qu'une mise en œuvre IPsec effectue un réassemblage/fragmentation IP supplémentaire afin, à la fois, de se conformer à la présente spécification, et de fournir une prise en charge IPsec transparente. Une attention particulière est nécessaire pour effectuer de telles opérations au sein de ces mises en œuvre lorsque plusieurs interfaces sont utilisées.)

En mode transport, ESP est inséré après l'en-tête IP et avant un en-tête de protocole de couche supérieure, par exemple, TCP, UDP, ICMP, etc. ou avant tous autres en-têtes IPsec qui auraient déjà été insérés. Dans le contexte de IPv4, ceci se traduit par le placement d'ESP après l'en-tête IP (et toutes options qu'il contient), mais avant le protocole de couche supérieure. (Noter que le terme mode "transport" ne devrait pas être interprété comme restreignant son utilisation à TCP et UDP. Par exemple, un message ICMP PEUT être envoyé en utilisant soit le mode "transport" soit le mode "tunnel".) Le diagramme suivant illustre le positionnement de mode transport ESP pour un paquet IPv4 typique, sur une base "avant et après". (La "queue d'ESP" accepte tous champs Bourrage, plus Longueur de bourrage, et Prochain en-tête.)



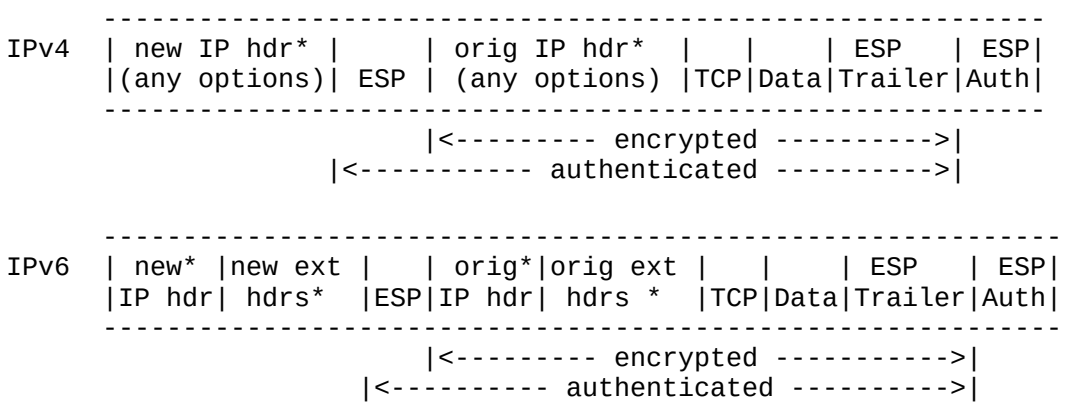
Dans le contexte IPv6, ESP est vu comme une charge utile de bout en bout, et donc devrait apparaître après les en-têtes d'extension de bond par bond, d'acheminement et de fragmentation. Le ou les en-têtes d'extension d'option de destination pourraient apparaître soit avant soit après l'en-tête ESP selon la sémantique désirée. Cependant, comme ESP protège seulement les champs après l'en-tête ESP, il peut généralement être souhaitable de placer le ou les en-têtes d'option de destination après l'en-tête ESP. Le diagramme suivant illustre le positionnement du mode transport ESP pour un paquet IPv6 typique.



* = s'il est présent, pourrait être avant ESP, après ESP, ou les deux.

Les en-têtes ESP et d'authentification peuvent être combinés dans divers modes. Le document d'architecture IPsec décrit les combinaisons d'associations de sécurité qui doivent être prises en charge.

Le mode tunnel ESP peut être employé dans les passerelles d'hôte ou de sécurité. Lorsque ESP est mis en œuvre dans une passerelle de sécurité (pour protéger le trafic de transit d'abonné), le mode tunnel doit être utilisé. En mode tunnel, l'en-tête IP "interne" porte les adresses ultimes de source et de destination, alors qu'une en-tête IP "externe" peut contenir des adresses IP distinctes, par exemple, les adresses des passerelles de sécurité. En mode tunnel, ESP protège le paquet IP interne tout entier, y compris l'en-tête IP interne tout entier. La position d'ESP en mode tunnel, par rapport à l'en-tête IP externe, est la même que pour ESP en mode transport. Le diagramme suivant illustre le positionnement d'ESP en mode tunnel pour des paquets IPv4 et IPv6 typiques.



* = s'il est présent, la construction des en-têtes /extensions IP externes et la modification des en-têtes /extensions IP internes est exposée ci-dessous.

3.2 Algorithmes

Les algorithmes de mise en œuvre obligatoire sont décrits à la Section 5, "Exigences de conformité". D'autres algorithmes PEUVENT être pris en charge. Noter que bien que la confidentialité et l'authentification soient toutes deux facultatives, au moins un de ces services DOIT être choisi et donc les deux algorithmes NE DOIVENT PAS être simultanément NULS.

3.2.1 Algorithmes de chiffrement

L'algorithme de chiffrement employé est spécifié par l'association de sécurité. ESP est conçu pour être utilisé avec des algorithmes de chiffrement symétriques. Parce que les paquets IP peuvent arriver en désordre, chaque paquet doit porter toutes les données nécessaires pour permettre au receveur d'établir la synchronisation cryptographique pour le déchiffrement. Ces données peuvent être portées explicitement dans le champ Charge utile, par exemple, comme un vecteur d'initialisation (comme décrit ci-dessus), ou les données peuvent être déduites de l'en-tête de paquet. Comme ESP a des dispositions pour le bourrage du texte en clair, les algorithmes de chiffrement employés avec ESP peuvent afficher des caractéristiques de mode

bloc ou flux. Noter que comme le chiffrement (confidentialité) est facultatif, cet algorithme peut être "NUL".

3.2.2 Algorithmes d'authentification

L'algorithme d'authentification employé pour le calcul d'ICV est spécifié par l'association de sécurité. Pour les communications point à point, les algorithmes d'authentification incluent les codes d'authentification de message (MAC) à clés fondés sur des algorithmes de chiffrement symétriques (par exemple, DES) ou sur des fonctions de hachage unidirectionnelles (par exemple, MD5 ou SHA-1). Pour les communications en multidiffusion, les algorithmes de hachage unidirectionnels combinés avec des algorithmes à signature asymétrique sont appropriés, bien que des considérations de performances et d'espace empêchent actuellement l'utilisation de tels algorithmes. Noter que comme l'authentification est facultative, cet algorithme peut être "NUL".

3.3 Traitement de paquet sortant

En mode transport, l'envoyeur incorpore les informations de protocole de couche supérieure dans l'en-tête/postambule ESP, et retient l'en-tête IP spécifié (et tous en-têtes d'extension IP dans le contexte IPv6). En mode tunnel, les en-têtes/extensions IP externes et internes peuvent être en interrelation de diverses façons. La construction des en-têtes/extensions IP externes durant le processus d'incorporation est décrite dans le document Architecture de sécurité. Si plus d'un en-tête/extension IPsec est requis par la politique de sécurité, l'ordre d'application des en-têtes de sécurité DOIT être défini par la politique de sécurité.

3.3.1 Vérification de l'association de sécurité

ESP ne s'applique à un paquet sortant qu'après qu'une mise en œuvre IPsec ait déterminé que le paquet est associé à une association de sécurité qui appelle un traitement ESP. Le processus de détermination du processus IPsec (s'il en est) qui s'applique au trafic sortant est décrit dans le document Architecture de sécurité.

3.3.2 Chiffrement de paquet

Dans ce paragraphe, on parle en termes de cryptage toujours appliqué à cause des implications de formatage. On doit comprendre que la "non confidentialité" est offerte par l'utilisation de l'algorithme de chiffrement NUL. En conséquence, l'envoyeur :

1. encapsule (dans le champ Charge utile ESP) :
   - pour le mode transport – seulement les informations originales de protocole de couche supérieure
   - pour le mode tunnel -- le datagramme IP d'origine tout entier.
2. ajoute tout bourrage nécessaire.

3. chiffre le résultat (données de charge utile, bourrage, longueur de bourrage et prochain en-tête) en utilisant la clé, l'algorithme de chiffrement, le mode d'algorithme indiqué par l'association de sécurité et les données de synchronisation cryptographiques (s'il en est).

- Si des données de synchronisation cryptographiques explicites, par exemple, un vecteur d'initialisation, sont indiquées, elles sont entrées dans l'algorithme de chiffrement selon la spécification d'algorithme et placées dans le champ Charge utile.
- Si des données de synchronisation cryptographiques implicites, par exemple, un vecteur d'initialisation, sont indiquées, elles sont construites et entrées dans l'algorithme de chiffrement conformément à la spécification de l'algorithme.

Les étapes exactes pour la construction de l'en-tête IP externe dépendent du mode (transport ou tunnel) et sont décrites dans le document Architecture de sécurité.

Si l'authentification est choisie, le chiffrement est effectué d'abord, avant l'authentification, et le chiffrement n'englobe pas le champ Données d'authentification. Cet ordre de traitement facilite la détection rapide et le rejet des paquets répétés ou lésés par le receveur, avant le déchiffrement du paquet, donnant par là la possibilité de réduire l'impact des attaques de déni de service. Cela donne aussi la possibilité d'un traitement parallèle des paquets chez le receveur, c'est-à-dire que le déchiffrement peut prendre place en parallèle à l'authentification. Noter que comme les Données d'authentification ne sont pas protégées par le chiffrement, un algorithme d'authentification chiffré doit être employé pour calculer l'ICV.

3.3.3 Génération de numéro de séquence

Le compteur de l'envoyeur est initialisé à 0 lors de l'établissement d'une association de sécurité. L'envoyeur incrémente le numéro de séquence pour cette association de sécurité et insère la nouvelle valeur dans le champ Numéro de séquence. Et donc le premier paquet envoyé en utilisant une association de sécurité données aura un numéro de séquence de 1.

Si l'anti-répétition est activée (par défaut, l'envoyeur le vérifie pour s'assurer que le compteur n'a pas fait un tour avant d'insérer la nouvelle valeur dans le champ Numéro de séquence. Autrement dit, l'envoyeur NE DOIT PAS envoyer un paquet sur une association de sécurité si cela doit provoquer un cycle de numéros de séquence. Une tentative de transmission d'un paquet qui aurait pour résultat un débordement du numéro de séquence est un événement contrôlable. (Noter que cette approche de la gestion des numéros de séquence n'exige pas l'utilisation d'une arithmétique modulaire.)

L'envoyeur suppose que l'anti-répétition est activée par défaut, à moins qu'il n'en soit notifié autrement par le receveur (voir le paragraphe 3.4.3). Et donc, si le compteur a fait un cycle, l'envoyeur va établir une nouvelle association de sécurité et de nouvelles clés (à moins que l'association de sécurité n'ait été configurée avec une gestion de clé manuelle).

Si l'anti-répétition est désactivée, l'envoyeur n'a pas besoin de surveiller le compteur ou de le remettre à zéro, par exemple, dans le cas de gestion de clé manuelle (voir la Section 5). Cependant, l'envoyeur incrémente toujours le compteur et lorsqu'il atteint la valeur maximale, le compteur revient à zéro.

3.3.4 Calcul de la valeur de la vérification d’intégrité

Si l’authentification est choisie pour l’association de sécurité, l’envoyeur calcule l’ICV sur le paquet ESP moins les données d’authentification. Et donc le SPI, le numéro de séquence, les données de charge utile, le bourrage (s’il est présent), la longueur de bourrage, et le prochain en-tête sont tous englobés dans le calcul d'ICV. Noter que les quatre derniers champs seront en forme chiffrée, car le chiffrement est effectué avant l’authentification.

Pour certains algorithmes d'authentification, la chaîne d’octets sur laquelle est effectué le calcul d'ICV doit être un multiple d’une taille de bloc spécifiée par l’algorithme. Si la longueur de cette chaîne d’octets ne correspond pas aux exigences de taille de bloc pour l’algorithme, le bourrage implicite NE DOIT PAS être ajouté à la fin du paquet ESP, (après le champ Prochain en-tête) avant le calcul d'ICV. Les octets de bourrage DOIVENT avoir une valeur de zéro. La taille de bloc (et donc la longueur du bourrage) est spécifiée par l’algorithme. Ce bourrage n’est pas transmis avec le paquet. Noter que MD5 et SHA-1 sont considérés comme ayant une taille de bloc de un octet à cause de leurs conventions de bourrage internes.

3.3.5 Fragmentation

Si nécessaire, la fragmentation est effectuée après le traitement ESP au sein d’une mise en œuvre IPsec. Et donc, le mode de transport ESP n’est appliqué qu’aux datagrammes IP complets (et pas aux fragments IP). Un paquet IP auquel ESP a été appliqué peut lui-même être fragmenté en chemin par les routeurs, et de tels fragments doivent être réassemblés avant le traitement ESP au receveur. En mode tunnel, ESP s’applique à un paquet IP, dont la charge utile peut être un paquet IP fragmenté. Par exemple, une passerelle de sécurité ou une mise en œuvre IPsec "prise dans la pile" ou "prise sur le réseau" (telles que définies dans le document Architecture de sécurité) peut appliquer le mode tunnel ESP à de tels fragments.

NOTE : Pour le mode transport -- comme mentionné au début du paragraphe 3.1, les mises en œuvre prises dans la pile et prises sur le réseau peut avoir d’abord à réassembler un paquet fragmenté par la couche IP locale, appliquer ensuite IPsec, puis à fragmenter le paquet résultant.

NOTE : Pour IPv6 -- pour les mises en œuvre prises dans la pile et prises sur le réseau, il sera nécessaire de passer à travers tous les en-têtes d’extension pour déterminer si il y a un en-tête de fragmentation et donc si le paquet a besoin d’être réassemblé avant le traitement IPsec.

3.4 Traitement de paquet entrant

3.4.1 Réassemblage

Si nécessaire, le réassemblage est effectué avant le traitement ESP. Si un paquet offert à ESP pour être traité se révèle être un fragment IP, c’est-à-dire que le champ OFFSET est différent de zéro ou que le fanion MORE FRAGMENTS est établi, le receveur DOIT éliminer le paquet ; ceci est un événement contrôlable. L’entrée d’enregistrement de contrôle pour cet

événement DEVRAIT inclure la valeur de SPI, la date/heure de réception, l'adresse de source, l'adresse de destination, le numéro de séquence, et (en IPv6) l'ID de flux.

NOTE : Pour le réassemblage de paquet, la spécification IPv4 actuelle N'EXIGE PAS de mettre à zéro le champ OFFSET ni l'élimination du fanion MORE FRAGMENTS. Afin de permettre le traitement IPsec d'un paquet réassemblé (au lieu de l'éliminer comme fragment apparent), le code IP doit effectuer ces deux tâches après le réassemblage d'un paquet.

3.4.2 Vérification d'association de sécurité

A réception d'un paquet (réassemblé) contenant un en-tête ESP, le receveur détermine l'association de sécurité appropriée (unidirectionnelle), sur la base de l'adresse IP de destination, du protocole de sécurité (ESP), et du SPI. (Ce processus est décrit plus en détails dans le document Architecture de sécurité.) L'association de sécurité indique si le champ Numéro de séquence sera vérifié, si le champ Données d'authentification devrait être présent, et si il va spécifier les algorithmes et clés à employer pour le déchiffrement et les calculs d'ICV (si applicable).

S'il n'existe pas d'association de sécurité valide pour cette session (par exemple, le receveur n'a pas de clé), le receveur DOIT écarter le paquet ; c'est un événement contrôlable. L'entrée d'enregistrement de contrôle pour cet événement DEVRAIT inclure la valeur de SPI, la date/heure de réception, l'adresse de source, l'adresse de destination, le numéro de séquence, et (en IPv6) l'ID de flux en texte clair.

3.4.3 Vérification de numéro de séquence

Toutes les mises en œuvre d'ESP DOIVENT prendre en charge le service anti-répétition, bien que son utilisation puisse être activée ou désactivée par le receveur ou association de sécurité par association de sécurité. Ce service NE DOIT PAS être activé si le service d'authentification n'est pas aussi activé pour l'association de sécurité, car autrement l'intégrité du champ Numéro de séquence n'est pas protégée. (Noter qu'il n'y a aucune disposition pour la gestion des valeurs de numéro de séquence émises entre plusieurs envoyeurs qui envoient du trafic à une seule association de sécurité (indépendamment du fait que l'adresse de destination soit en monodiffusion, en diffusion générale ou en diffusion groupée). Et donc, le service anti-répétition NE DEVRAIT PAS être utilisé dans un environnement multi envoyeurs qui utilise une seule association de sécurité.)

Si le receveur n'active pas l'anti-répétition pour une association de sécurité, aucune vérification à l'entrée n'est effectuée sur le numéro de séquence. Cependant, du point de vue de l'envoyeur, la position par défaut est de supposer que l'anti-répétition est activée chez le receveur. Pour éviter que l'envoyeur n'effectue une surveillance de numéro de séquence et un établissement d'association de sécurité inutiles (voir au paragraphe 3.3.3), si un protocole d'établissement d'association de sécurité tel que IKE est utilisé, le receveur DEVRAIT notifier à l'envoyeur, durant l'établissement de l'association de sécurité, si il ne va pas fournir la protection anti-répétition.

Si le receveur a activé le service anti-répétition pour cette association de sécurité, le compteur de paquets reçus pour l'association de sécurité DOIT être initialisé à zéro lorsque l'association

de sécurité est établie. Pour chaque paquet reçu, le receveur DOIT vérifier que le paquet contient un numéro de séquence qui ne duplique pas le numéro de séquence de tout autre paquet reçu pendant la durée de vie ce cette association de sécurité. Ceci DEVRAIT être la première vérification d'ESP appliquée à un paquet après sa comparaison avec une association de sécurité, pour accélérer le rejet des paquets dupliqués.

Les duplicata sont rejetés au moyen de l'utilisation d'une fenêtre glissante de réception. (La façon de mettre en œuvre la fenêtre est une question locale, mais le texte qui suit décrit les fonctions que la mise en œuvre doit offrir.) Une taille MINIMUM de fenêtre de 32 DOIT être acceptée ; mais une taille de fenêtre de 64 est préférée et DEVRAIT être employée par défaut.

Une autre taille de fenêtre (plus grande que le MINIMUM) PEUT être choisie par le receveur. (Le receveur NE notifie PAS la taille de fenêtre à l'envoyeur.)

Le bord "droit" de la fenêtre représente la plus forte valeur validée de numéro de séquence reçue sur cette association de sécurité. Les paquets qui contiennent des numéros de séquence inférieurs à ceux du bord "gauche" de la fenêtre sont rejetés. Les paquets qui tombent dans la fenêtre sont comparés à une liste des paquets reçus dans la fenêtre. Un moyen efficace d'effectuer cette vérification, sur la base de l'utilisation d'un gabarit binaire, est décrit dans le document Architecture de sécurité.

Si le paquet reçu tombe dans la fenêtre et est nouveau, ou si le paquet est à la droite de la fenêtre, le receveur procède à la vérification d'ICV. Si la validation d'ICV échoue, le receveur DOIT écarter le datagramme IP reçu comme invalide ; ceci est un événement contrôlable. L'entrée d'enregistrement de contrôle DEVRAIT inclure la valeur de SPI, la date/heure de réception, l'adresse de source, l'adresse de destination, le numéro de séquence, et (en IPv6) l'ID de flux. La fenêtre de réception n'est mise à jour que si la vérification d'ICV réussit.

DISCUSSION :
Noter que si le paquet est dans la fenêtre et est nouveau, ou s'il est en-dehors de la fenêtre sue le côté "droit", le receveur DOIT authentifier le paquet avant de mettre à jour les données de la fenêtre de numéro de séquence.

3.4.4 Calcul de la valeur de vérification d'intégrité

Si l'authentification a été choisie, le receveur calcule l'ICV sur le paquet ESP moins les données d'authentification en utilisant l'algorithme d'authentification spécifié et vérifie que c'est le même que l'ICV inclus dans le champ Données d'authentification du paquet. Les détails du calcul sont donnés ci-dessous.

Si l'ICV calculé et celui reçu concordent, le datagramme est alors valide, et il est accepté. Si l'essai échoue, le receveur DOIT alors écarter le datagramme IP reçu comme invalide ; ceci est un événement contrôlable. Les données d'enregistrement DEVRAIENT inclure la valeur de SPI, la date/heure de réception, l'adresse de source, l'adresse de destination, le numéro de séquence, et (en IPv6) l'ID de flux en texte clair.

DISCUSSION :
Commencer par retirer et sauvegarder la valeur de l'ICV (champ de données d'authentification). Vérifier ensuite la longueur totale du paquet ESP moins les données

d’authentification. Si le bourrage implicite est requis, sur la base de la taille de bloc de l’algorithme d'authentification, ajouter des octets remplis de zéros à la fin du paquet ESP directement après le champ Prochain en-tête. Effectuer le calcul d'ICV et comparer le résultat à la valeur sauvegardée, en utilisant les règles de comparaison définies par la spécification de l’algorithme. (Par exemple, si une signature numérique et un hachage unidirectionnel sont utilisés pour le calcul d'ICV, le processus de confrontation est plus complexe.)

3.4.5 Déchiffrement de paquet

Comme dans le paragraphe 3.3.2, "Chiffrement de paquet", on parle ici en termes de chiffrement toujours appliqué à cause des implications de formatage. Ceci est fait en sous-entendant que la "non confidentialité" est offerte par l’utilisation de l’algorithme de chiffrement NULL.
En conséquence, le receveur :

1. déchiffre les données de charge utile d’ESP, le bourrage, la longueur de bourrage, et le Prochain en-tête en utilisant la clé, l’algorithme de chiffrement, le mode d’algorithme, et les données de synchronisation cryptographiques (s’il en est), indiqués par l’association de sécurité.
   - Si des données de synchronisation cryptographiques explicites, par exemple, un vecteur d'initialisation, sont indiquées, elles sont tirées du champ Charge utile et entrées dans l’algorithme de déchiffrement conformément à la spécification de l’algorithme.
   - Si des données de synchronisation cryptographiques implicites, par exemple, un vecteur d'initialisation, sont indiquées, une version locale du vecteur d'initialisation est construite et entrée dans l’algorithme de déchiffrement conformément à la spécification de l’algorithme.
2. traite tout bourrage comme spécifié dans la spécification de l’algorithme de chiffrement. Si le schéma de bourrage par défaut (voir au paragraphe 2.4) a été utilisé, le receveur DEVRAIT inspecter le champ Bourrage avant de retirer le bourrage et de passer les données déchiffrées à la couche suivante.
3. reconstruire le datagramme IP original à partir de :
   - pour le mode transport – l’en-tête IP d’origine plus les informations originales de protocole de couche supérieure dans le champ Charge utile d’ESP.
   - pour le mode tunnel – de l’en-tête IP de tunnel + le datagramme IP entier dans le champ Charge utile d’ESP.

Les étapes exactes pour la reconstruction du datagramme original dépendent du mode (transport ou tunnel) et sont décrites dans le document Architecture de sécurité. Au minimum, dans un contexte IPv6, le receveur DEVRAIT s’assurer que les données déchiffrées sont verrouillées sue huit octets, pour faciliter le traitement par le protocole identifié dans le champ Prochain en-tête.

Si l’authentification a été choisie, la vérification et le déchiffrement PEUVENT être effectués en série ou en parallèle. Si elles sont effectuées en série, la vérification d’ICV DEVRAIT alors être effectuée en premier. Si elles sont effectuées en parallèle, la vérification DOIT être achevée avant que le paquet déchiffré soit passé à l’étape de traitement suivante. Cet ordre de traitement facilite la détection et le rejet rapides des paquets répétés ou lésés par le receveur, avant le déchiffrement du paquet, et donc, cela peut réduire l’impact d’attaques de déni de service. Note : Si le receveur effectue le déchiffrement en parallèle avec l’authentification, il

faut veiller à éviter une possible compétition antre l'accès au paquet et la reconstruction du paquet déchiffré.

Noter qu'il y a plusieurs façons pour l'"échec" du déchiffrement :

a. L'association de sécurité choisie peut n'être pas correcte – L'association de sécurité peut être mal choisie du fait d'une altération du SPI, de l'adresse de destination, ou des champs de type de protocole IPsec. De telles erreurs, si elles transposent le paquet à une autre association de sécurité existante, seront indistinguables d'un paquet corrompu, (cas c). L'altération du SPI peut être détectée en utilisant l'authentification. Cependant, une non concordance d'association de sécurité peut aussi survenir du fait de l'altération de l'adresse de destination IP ou du champ de type de protocole IPsec.
b. La longueur de bourrage ou les valeurs de bourrage pourraient être erronées – De mauvaises longueurs de bourrage ou de valeurs de bourrage peuvent être détectées indépendamment de l'utilisation de l'authentification.
c. Le paquet ESP chiffré pourrait être corrompu – Ceci peut être détecté si l'authentification est choisie pour l'association de sécurité.

Dans les cas (a) ou (c), le résultat erroné de l'opération de déchiffrement (un datagramme IP ou une trame de couche transport invalide) ne sera pas nécessairement détecté par IPsec, et relève du traitement du protocole suivant.

4. Inspection

Tous les systèmes qui mettent en œuvre ESP n'appliquent pas le contrôle. Cependant, si ESP est incorporé dans un système qui prend en charge le contrôle, la mise en œuvre ESP DOIT alors aussi prendre en charge le contrôle et DOIT permettre à un administrateur de système d'activer ou désactiver le contrôle pour ESP. Pour la plus grande part, la granularité du contrôle est une affaire locale. Cependant, plusieurs événements contrôlables sont identifiés dans la présente spécification et pour chacun de ces événements un ensemble minimum d'informations qui DEVRAIENT être incluses dans un enregistrement de contrôle est défini. Des informations supplémentaires PEUVENT aussi être incluses dans l'enregistrement de contrôle pour chacun de ces événements, et des événements supplémentaires, non spécifiquement énumérés dans la présente spécification, PEUVENT aussi déboucher sur des entrées d'enregistrements de contrôle. Il n'est pas exigé du receveur de transmettre de message à l'envoyeur prétendu en réponse à la détection d'un événement contrôlable, à cause du potentiel de déni de service induit via une telle action.

5. Exigences de conformité

Les mises en œuvre qui se réclament de la conformité à la présente spécification DOIVENT mettre en œuvre la syntaxe ESP et le traitement décrit ici et DOIVENT se conformer à toutes les exigence du document Architecture de sécurité. Si la clé utilisée pour calculer un ICV est distribuée manuellement, une disposition correcte du service d'anti-répétition exigerait une maintenance correcte de l'état du compteur chez l'envoyeur, jusqu'à ce que la clé soit remplacée, et il n'y aura vraisemblablement pas de dispositif de récupération automatique si le débordement du compteur est imminent. Et donc une mise en œuvre conforme NE DEVRAIT PAS fournir ce service en conjonction avec des associations de sécurité qui sont

entrées manuellement. Une mise en œuvre ESP conforme DOIT prendre en charge les algorithmes de mise en œuvre obligatoire suivants :

- DES en mode CBC [MD97]
- HMAC avec MD5 [MG97a]
- HMAC avec SHA-1 [MG97b]
- Algorithme d'authentification NULL
- Algorithme de chiffrement NULL

Comme le chiffrement et l'authentification ESP sont facultatifs, la prise en charge des deux algorithmes "NULL" est exigée pour maintenir la cohérence avec la façon dont ces services sont négociés. NOTER qu'alors que l'authentification et le chiffrement peuvent chacun être "NULL", ils ne DOIVENT PAS être "NULL" tous les deux.

6. Considérations sur la sécurité

La sécurité est une question centrale dans la conception du présent protocole, et donc les considérations de sécurité imprègnent cette spécification. Des aspects supplémentaires en rapport avec la sécurité pour l'utilisation du protocole IPsec sont exposés dans le document Architecture de sécurité.

7. Différences avec la RFC 1827

Le présent document diffère de la RFC 1827 [ATK95] de plusieurs façons significatives. La différence majeure est que le présent document essaye de spécifier un cadre et un contexte complet pour ESP, tandis que la RFC 1827 fournissait une "coquille" qui était complétée par la définition d'amendements. La croissance combinatoire des amendements a motivée la reformulation de la spécification d'ESP sous forme d'un document plus complet, avec des options pour les services de sécurité qui peuvent être offerts dans le contexte d'ESP. Et donc, les champs précédemment définis dans les documents d'amendement font maintenant partie de la spécification ESP de base. Par exemple, les champs nécessaires à la prise en charge de l'authentification (et de l'anti-répétition) y sont maintenant définis, même si la fourniture de ce service est une option. Les champs utilisés pour la prise en charge du bourrage pour le chiffrement, et pour identification du protocole suivant, y sont maintenant aussi définis. Le traitement des paquets cohérent avec la définition de ces champs est aussi inclus dans le document.

Remerciements

De nombreux concepts incorporés dans la présente spécification sont tirés du protocole de sécurité SP3 du Gouvernement américain, du NLSP de l'ISO/CEI ou influencés par eux, ou par le protocole de sécurité proposé swIPe. [SDNS89, ISO92, IB93].

Durant près de trois ans, ce document a évolué à travers de multiples versions et itérations. Pendant ce temps, de nombreuses personnes ont contribué par des idées significatives et leur énergie au processus et aux documents eux-mêmes. Les auteurs remercient particulièrement Karen Seo pou son aide précieuse dans la révision, l'édition, les recherches de base et la

coordination de cette version de la spécification. Les auteurs remercient également les membres des groupes de travail IPsec et IPng, avec une mention particulière pour les efforts de (en ordre alphabétique) : Steve Bellovin, Steve Deering, Phil Karn, Perry Metzger, David Mihelcic, Hilarie Orman, Norman Shulman, William Simpson et Nina Yuan.

Références

[ATK95] Atkinson, R., "IP Encapsulating Security Payload (ESP)" *(Incorporation de charge utile de sécurité sur IP (ESP))*, RFC 1827, août 1995.

[Bel96] Steven M. Bellovin, "Problem Areas for the IP Security Protocols" *(Circonscription des problèmes pour les protocoles de sécurité IP)*, Procés verbaux du sixième Usenix Unix Security Symposium, juillet 1996.

[Bra97] Bradner, S., "Mots clés à utiliser dans les RFC pour indiquer les niveaux d’exigence", BCP 14, RFC 2119, mars 1997.

[HC98] Harkins, D., et D. Carrel, "The Internet Key Exchange (IKE)" *(Echange de clés Internet)*, RFC 2409, novembre 1998.

[IB93] John Ioannidis & Matt Blaze, "Architecture and Implementation of Network-layer Security Under Unix" *(Architecture et mise en œuvre de la sécurité de la couche réseau sous Unix)*, Procés verbaux du USENIX Security Symposium, Santa Clara, CA, octobre 1993.

[ISO92] ISO/CEI JTC1/SC6, Protocole de sécurité de la couche réseau, ISO-CEI DIS 11577, International Standards Organisation, Genève, Suisse, 29 novembre 1992.

[KA97a] Kent, S., et R. Atkinson, "Security Architecture for the Internet Protocol" *(Architectue de sécurité pour le protocole Internet)*, RFC 2401, novembre 1998.

[KA97b] Kent, S., et R. Atkinson, "IP authentication header" *(En-tête d'authentification IP)*, RFC 2402, novembre 1998.

[MD97] Madson, C., et N. Doraswamy, "The ESP DES-CBC Cipher Algorithm With Explicit vecteur d'initialisation", RFC 2405, novembre 1998.

[MG97a] Madson, C., et R. Glenn, "The Use of HMAC-MD5-96 within ESP and authentication header" (*Utilisation de HMAC-MD5-96 dans ESP et un en-tête d'authentification)*, RFC 2403, novembre 1998.

[MG97b] Madson, C., et R. Glenn, "The Use of HMAC-SHA-1-96 within ESP and authentication header" *(Utilisation de HMAC-SHA-1-96 dans ESP et un en-tête d'authentification)*, RFC 2404, novembre 1998.

[STD-2] Reynolds, J., et J. Postel, "Assigned Numbers" *(Numéros alloués)*, STD 2, RFC 1700, octobre 1994. Voir aussi : http://www.iana.org/numbers.html

[SDNS89] SDNS Secure Data Network System, Security Protocol 3, SP3, *(SDNS, Système réseau de données sécurisées, Protocole de sécurité 3, SP3)* Document SDN.301, Révision 1.5, 15 mai 1989, tel que publié dans NIST Publication NIST-IR-90-4250, février 1990.

Décharge de responsabilité

Les opinions et spécification présentées ici sont celles des auteurs et ne sont pas nécessairement celles de leurs employeurs. Les auteurs et leurs employeurs déclinent spécifiquement toute responsabilité pour les problèmes survenant d'une mise en œuvre correcte ou incorrecte ou de l'utilisation de la présente spécification.

Adresse des auteurs

Stephen Kent	Randall Atkinson
BBN Corporation	@Home Network
70 Fawcett Street	425 Broadway,
Cambridge, MA 02140	Redwood City, CA 94063
USA	USA
tél : +1 (617) 873-3988	tél : +1 (415) 569-5000
mél : kent@bbn.com	mél : rja@corp.home.net

Déclaration complète de Copyright