Groupe de travail Réseau
Request for Comments : 5406
BCP 146
Catégorie : Bonne pratiques actuelles

S. Bellovin, Columbia University
février 2009

Traduction Claude Brière de L'Isle

Lignes directrices pour spécifier l'utilisation de IPsec version 2

Résumé
La section des considérations sur la sécurité de nombreux projets Internet dit juste, en effet, "utiliser IPsec". Bien que ceci soit parfois correct, plus souvent cela laisse les utilisateurs sans mécanisme de sécurité réel, interopérable. Le présent mémoire offre des lignes directrices sur quand IPsec version 2 devrait er ne devrait pas être spécifié.

Table des matières

1. Introduction

Les sections des considérations sur la sécurité de nombreux projets Internet disent juste en effet, "utiliser IPsec". Bien que l'utilisation de IPsec soit parfois la solution de sécurité correcte, plus d'information est nécessaire pour fournir des solutions de sécurité interopérables. Dans certains cas, IPsec est indisponible dans les points d'extrémité attendus. Si IPsec est indisponible pour -- et donc inutilisable par -- une majorité des utilisateurs dans un environnement de protocole particulier, alors la spécification de IPsec est équivalente à dire "débrancher la sécurité" au sein ce cette communauté. De plus, quand IPsec est disponible, la mise en œuvre peut ne pas fournir la granularité de protection appropriée. Finalement, si IPsec est disponible et approprié, le document qui rend obligatoire l'utilisation de IPsec doit spécifier juste comment il doit être utilisé.

Le but de ce document est de donner des lignes directrices aux concepteurs de protocoles sur la spécification de IPsec quand il est le mécanisme de sécurité approprié. La spécification de protocole est supposée donner une sécurité réaliste, interopérable. Donc, des directives sur la configuration des diverses bases de données IPsec, comme la base de données de politique de sécurité (SPD, *Security Policy Database*) sont souvent requises.

Le présent document décrit comment spécifier l'utilisation de IPsec version 2 [RFC2401] y compris de la version 2 de l'encapsulation de charge utile de sécurité (ESPv2, *Encapsulating Security Payload version 2*) [RFC2406], de la version 2 de l'en-tête d'authentification (AHv2, *Authentication Header version 2*) [RFC2402], et de la version 1 de l'échange de clés Internet (IKEv1, *Internet Key Exchange version 1*) [RFC2409]. Un document séparé décrira la suite IPsec version 3 [RFC4301] [RFC4302] [RFC4303] [RFC4306].

Pour plus d'indications sur les considérations sur la sécurité (y compris la discussion de IPsec) voir la [RFC3552].

Note : beaucoup des arguments ci-dessous se rapportent aux capacités des mises en œuvre actuelles de IPsec. Elles peuvent changer au fil du temps ; cet avis se fonde sur les connaissances disponibles à l'IETF au moment de la publication.

2. Avertissement

La conception de protocoles de sécurité est un art subtil et difficile. Les avertissements donnés ici sur la façon de spécifier l'utilisation de IPsec NE devraient PAS être pris comme signifiant qu'on devrait inventer son propre protocole de sécurité pour chaque nouvelle application. Si IPsec est un mauvais choix, utiliser un autre protocole de sécurité normalisé, bien compris, va presque toujours donner les meilleurs résultats pour la mise en œuvre et le déploiement. Les protocoles de sécurité sont très difficiles à concevoir ; en enrôler un nouveau va exiger un travail théorique et pratique extensif pour confirmer ses propriétés de sécurité et va entraîner des délais et des incertitudes.

3. Composants d'IPsec

IPsec est composé de plusieurs pièces différentes. Elles peuvent être utilisées pour fournir la protection de la confidentialité, de l'intégrité, et contre la répétition ; bien que certaines puissent être configurées manuellement, un composant de gestion clé est généralement utilisé. De plus, la décision de si et comment utiliser IPsec est contrôlée par une sorte de base de données de politiques.

3.1 AH et ESP

L'en-tête d'authentification (AH, *Authentication Header*) [RFC2402] et la charge utile de sécurité encapsulante (ESP, *Encapsulating Security Payload*) [RFC2406] sont les protocoles de sécurité sur le réseau. Tous deux fournissent la protection contre la répétition (facultative). ESP est normalement utilisé pour fournir la confidentialité (chiffrement) l'intégrité, et l'authentification au trafic. ESP peut aussi fournir l'intégrité et l'authentification sans la confidentialité, ce qui en fait une bonne solution de remplacement de AH dans la plupart des cas où la confidentialité n'est pas un service exigé ou désiré. Finalement, ESP peut être utilisé pour fournir la seule confidentialité, bien que ce ne soit pas recommandé [Bell96].

La différence de protection de l'intégrité offerte par AH est que AH protège des portions de l'en-tête IP précédant, incluant l'adresse de source et de destination. Cependant, si ESP est utilisé en mode tunnel (voir le paragraphe 3.2) et si

l'intégrité/authentification est activée, l'en-tête IP vu par les hôtes de source et destination est complètement protégé de toutes façons.

AH peut aussi protéger les options IP qui doivent être vues par les routeurs intermédiaires, mais doit être intact et authentique quand il est livré au système receveur. Pour l'instant, l'utilisation (et l'existence) de telles options IP est extrêmement rare.

Si une application exige une telle protection, et si les informations à protéger ne peuvent pas être déduites du processus de gestion de clés, AH doit être utilisé. (ESP est généralement considéré comme plus facile à mettre en œuvre ; cependant, virtuellement tous les paquetages IPsec prennent les deux en charge.) Si la confidentialité est demandée, ESP doit être utilisé. Il est possible d'utiliser AH conjointement avec ESP, mais cette combinaison est rarement exigée.

Toutes les variantes de IPsec ont des problèmes avec les boîtiers de NAT – voir les détails dans la [RFC3715] -- mais AH est considérablement plus perturbateur. Dans les environnements où il y a une forte probabilité que les deux points d'extrémité soient séparés par un boîtier de NAT -- cela inclut presque tous les services impliquant un trafic d'utilisateur à serveur, par opposition à du trafic de serveur à serveur – la traversée de NAT [RFC3948] devrait être rendue obligatoire et AH devrait être évité. (Noter que la [RFC3948] est seulement pour ESP, et ne peut être utilisée pour AH.)

3.2 Mode transport et mode tunnel

AH et ESP peuvent tous deux être utilisés en mode transport ou en mode tunnel. En mode tunnel, l'en-tête IPsec est suivi par un en-tête IP interne. C'est l'usage normal pour les réseaux virtuels privés (VPN, *Virtual Private Network*) et est généralement exigé chaque fois que l'une ou l'autre des extrémité du chemin protégé par IPsec n'est pas la destination IP ultime, par exemple, quand IPsec est mis en œuvre dans un pare-feu, un routeur, etc.

Le mode transport est préféré pour les communications en point à point, bien que le mode tunnel puisse aussi être utilisé à cette fin.

3.3 Gestion de clé

Tout système cryptographique exige la gestion des clés. IPsec assure des schémas de gestion de clé manuels et automatiques. La gestion de clé manuelle est aisée ; cependant, elle ne s'adapte pas très bien. Aussi, les mécanismes de protection contre la répétition de IPsec ne sont pas disponibles si la gestion de clé manuelle est utilisée. Le besoin d'un échange automatique de clés est discuté plus en détails dans la [RFC4107].

Le principal mécanisme automatisé d'échange de clés pour IPsec est l'échange de clé Internet (IKE, *Internet Key Exchange*) [RFC2409]. Une nouvelle version de IKE plus simple, a été approuvée [RFC4306], mais de nombreux systèmes existants utilisent encore IKEv1. Le présent document ne discute pas de IKEv2 et IPsecv3. Un second mécanisme, négociation de clé Internet kerbérisée (KINK, *Kerberized Internet Negotiation of Keys*) [RFC4430], a été défini. Il utilise bien sûr Kerberos et ne convient que si et seulement si une infrastructure Kerberos est disponible.

Si la décision d'utiliser IKE est prise, le mode de fonctionnement précis doit aussi être spécifié. IKE peut être utilisé en mode principal ou en mode aggressif ; tous deux prennent en charge les signatures numériques, deux façons différentes d'utiliser le chiffrement de clé publique, et les secrets partagés pour l'authentification.

L'authentification par secret partagé est plus simple ; cependant, elle ne s'adapte pas très bien dans les scénarios de communication de plusieurs à plusieurs parce que chaque point d'extrémité doit partager un secret unique avec chaque homologue avec lequel il peut communiquer. Noter cependant qu'utiliser des secrets partagés dans IKE est de loin préférable au chiffrement manuel.

Dans la plupart des situations où les modes de clé publique de IKE sont utilisés, des certificats produits en local sont employés. C'est-à-dire, l'administrateur du système ou du réseau concerné va produire des certificats à tous les utilisateurs autorisés. Ces certificats ne sont utiles que pour IPsec.

Il est parfois possible d'utiliser des certificats [RFC5280] provenant d'une infrastructure existante de clé publique (PKI, *Public Key Infrastructure*) avec IKE. En pratique, c'est rare. De plus, non seulement il n'y a pas de PKI globale couvrant la plupart des points d'extrémité Internet, et il n'y en aura probablement jamais. Concevoir une structure qui suppose une telle PKI est une faute. En particulier, supposer qu'un nœud arbitraire aura un certificat "authentique", produit par un tiers

mutuellement de confiance et attestant de l'identtité de ce nœud, est faux. Là encore, une telle PKI n'esiste pas et n'existera probablement jamais. L'IKE de clé publique est généralement une bonne idée, mais devrait presque toujours être utilisé avec des certificats produits en local par opposition à des certificats provenant d'une PKI existante.

Noter que les schémas de clé publique exigent une quantité de calcul substantielle. Les concepteurs de protocoles devraient examiner si de tels calculs sont ou non faisables sur les appareils qui intéressent leur clientèle. Utiliser des certificats double en gros le nombre de grandes exponentiations qui doivent être effectuées, par rapport aux versions à secret partagé de IKE.

Aujourd'hui, même les appareils à faible puissance peuvent généralement effectuer assez de calcul pour établir un nombre limité d'associations de sécurité. Les points de concentration, comme les pare-feu ou les serveurs VoIP, peuvent demander une assistance matérielle, en particulier si de nombreux homologues sont supposés créer des associations de sécurité à peu près au même moment.

Utiliser un mécanisme de gestion automatique de clés peut être difficile quand on essaye de protéger des protocoles de bas niveau. Par exemple, bien que la [RFC2461] ait spécifié l'utilisation de IPsec pour protéger la découverte de voisin IPv6, il a été impossible de faire la gestion de clés : les nœuds ne pouvaient pas utiliser IKE parce qu'il exige une communication de niveau IP, et que ce n'est pas possible avant l'établissement d'associations de découverte de voisin.

3.4 Interface de programmation d'application (API)

C'est, dans un certain sens, un abus de langage de parler de l'API comme d'une partie d'IPsec car cette pièce est manquante dans beaucoup de systèmes. Dans la mesure où des API existent, elles ne sont pas normalisées. Le problème est simple : il n'y a pas de moyen portable (et souvent pas de moyen du tout) pour une application de demander la protection IPsec, ou de dire si elle a été utilisée pour des paquets ou connexions entrants donnés.

Il y a des problèmes supplémentaires :

- Les applications ont rarement accès à de telles API. IPsec est plutôt configuré généralement par un administrateur de système ou de réseau.

- Les applications ne sont pas capables de vérifier que des services IPsec sont utilisés en dessous.

- Les applications ne connaissent pas les identités et propriétés spécifiques du canal protégé fourni par IPsec. Par exemple, les mécanismes de gestion de clé IPsec peuvent être avertis de l'identité et de l'autorisation de l'homologue, mais cette information ne peut pas être utilisée par l'application ni reliée aux décisions de niveau application, comme l'accès aux ressources réservées à l'entité identifiée par cette identité.

Les mises en œuvre IPsec fondées sur un routeur ou un pare-feu posent des problèmes encore plus grands parce qu'il n'y a pas de protocole réseau normalisé pour communiquer aux hôtes ces informations à partir des chiffreurs externes.

À l'opposé, des services de sécurité de couche supérieure, comme TLS, sont capables de fournir le contrôle et l'assurance nécessaires.

4. Disponibilité de IPsec dans les appareils cibles

Bien que IPsec soit maintenant largement mis en œuvre et soit disponible pour les livraisons actuelles de la plupart des systèmes d'exploitation d'hôtes, il est moins disponible pour les systèmes incorporés. Peu de concentrateurs, de traducteurs d'adresse réseau, etc., le mettent en œuvre, en particulier à l'extrémité inférieure. Il est généralement inapproprié de s'appuyer sur IPsec quand de nombreux points d'extrémité sont dans cette catégorie.

Même pour une utilisation d'hôte à hôte, la disponibilité d'IPsec (et l'expérience et facilité d'utilisation) a généralement été pour des VPN. Les hôtes qui prennent en charge IPsec pour une utilisation de VPN ne le prennent fréquemment pas en charge en point à point, en particulier via une API stable, bien définie ou une interface d'utilisateur.

Finalement, peu de mises en œuvre prennent en charge plusieurs couches d'IPsec. Si un télécommuniquant utilise IPsec en mode VPN pour accéder à un réseau d'organisation, il peut n'être pas capable d'employer un second niveau de IPsec pour

protéger une connexion d'application à un hôte au sein de l'organisation. (On note qu'une telle prise en charge est, en fait, rendue obligatoire par le cas 4 du paragraphe 4.5 de la [RFC2401]. Néanmoins, il n'est pas largement disponible.) La probabilité de tels scénarios de déploiement devrait être prise en compte quand on décide si IPsec est ou non rendu obligatoire.

5. Points d'extrémité

La [RFC2401] décrit de nombreuses formes différentes d'identifiant de point d'extrémité. Cela inclut les adresses de source (IPv4 et IPv6) les noms d'hôte (éventuellement comme étant incorporés dans des certificats X.500) et des identifiants d'utilisateur (là encore, éventuellement incorporés dans un certificat). Toutes les formes d'identifiant ne sont pas disponibles sur toutes les mises en œuvre ; en particulier, l'identification à la granularité d'utilisateur n'est pas courante. Ceci est en particulier un problème pour les systèmes multi-utilisateurs, où il peut n'être pas possible d'utiliser des certificats différents pour distinguer le trafic provenant de deux utilisateurs différents.

Là encore, on note que la capacité de fournir une protection de granularité fine, comme de chiffrer chaque connexion séparement et avec des accréditifs par utilisateur, était un des buts originaux de la conception de IPsec. Néanmoins, seulement quelques plate-formes le prennent en charge. Bien sûr, certaines mises en œuvre ne prennent même pas en charge l'utilisation des numéros d'accès quand elles décident si elles appliquent ou non la protection IPsec.

6. Sélecteurs et SPD

Le paragraphe 4.4 de la [RFC2401] décrit la base de données de politique de sécurité (SPD, *Security Policy Database*) et les "sélecteurs" utilisés pour décider quel trafic devrait être protégé par IPsec. Les choix incluent les adresses de source et destination (ou gammes d'adresses) les numéros de protocole (c'est-à-dire, 6 pour TCP et 17 pour UDP) et les numéros d'accès pour TCP et UDP. Les protocoles dont les exigences de protection ne peuvent pas être décrites dans ces termes sont de mauvais candidats pour IPsec ; en particulier, il devient impossible d'appliquer la protection à une granularité plus fine que "hôte de destination". Donc, le trafic incorporé dans une session de protocole de tunnelage de couche 2 (L2TP, *Layer 2 Tunneling Protocol*) [RFC2661] ne peut pas être protégé de façon sélective par IPsec au dessus de la couche L2TP, parce que IPsec n'a pas de sélecteurs définis, ce qui laisse son homologue dans le paquet L2TP trouver les numéros d'accès TCP. De même, le protocole de transmission de commandes de flux (SCTP, *Stream Control Transmission Protocol*) [RFC4960] n'existait pas quand la [RFC2401] a été rédigée ; donc, protéger les applications SCTP individuelles sur la base du numéro d'acccès ne pouvait pas être fait avant qu'un nouveau document soit écrit, la [RFC3554] qui définissait de nouveaux sélecteurs pour IPsec, et des mises en œuvre sont apparues.

De plus, dans un monde qui s'appuie dans une large mesure sur une allocation dynamique des adresses et utilise souvent aussi des numéros d'accès alloués dynamiquement, une politique de tout ou rien pour les VPN peut fonctionner correctement ; d'autres politiques peuvent cependant être difficiles à créer sous une forme utilisable.

La granularité de protection disponible peut avoir des effets collatéraux. Si certain trafic entre une paire de machines est protégé par IPsec, la mise en œuvre permet elle que d'autre trafic soit non protégé ou protégé par des politiques différentes ? Autrement, si la mise en œuvre est telle qu'elle soit seulement capable de protéger tout le trafic ou aucun, l'appareil a t-il une capacité de CPU suffisante pour tout chiffrer ? Noter que certains appareils d'extrémité inférieure peuvent avoir une capacité de mémorisation sûre limitée pour les clés, etc.

Les problèmes de mise en œuvre sont aussi un souci ici. Comme précédemment, trop de fabricants n'ont pas mis en œuvre la spécification complète ; trop de mises en œuvre IPsec ne sont pas capables d'utiliser les numéros d'accès dans leurs sélecteurs. La protection du trafic entre deux hôtes est donc un tout ou rien quand ces mises en œuvre non conformes sont employées.

7. Diffusion et diffusion groupée

Bien que les concepteurs de IPsec aient essayé de laisser de la place pour la protection du trafic de diffusion groupée, la conception complète n'a été terrminée que beaucoup plus tard. C'est pour cela que de nombreuses mises en œuvre de IPsec ne prennent pas en charge la diffusion groupée. La [RFC5374] décrit des extensions à IPsec pour la prendre en charge. Les

autres documents pertinents incluent les [RFC3830], [RFC3547], et [RFC4535].

À cause du délai, les concepteurs de protocoles qui utilisent la diffusion groupée devraient examiner la disponibilité de ces extensions dans les plates-formes intéressantes.

8. Spécifier IPsec

En dépit de tous les avertissements donnés ci-dessus, il peut quand même être approprié d'utiliser IPsec dans des situations particulières. La gamme des choix rend obligatoire de définir précisément comment IPsec va être utilisé. Les auteurs de documents de normalisation qui s'appuient sur IPsec doivent spécifier ce qui suit :

a. Quels sélecteurs devrait utiliser l'initiateur de la conversation (le client, dans les architectures client-serveur) ? Quelles adresses, numéros d'accès, etc., sont à utiliser ?

b. Quel protocole IPsec est à utiliser : AH ou ESP ? Quel mode est à employer : mode transport ou mode tunnel ?

c. Quelle forme de gestion de clé est appropriée ?

d. Quelle forme d'identification devrait être utilisée ? Les choix incluent l'adresse IP, le nom DNS avec ou sans un nom d'utilisateur, et le nom distinctif X.500.

e. Si le serveur d'application va commuter les identifiants d'utilisateur (c'est-à-dire, c'est une sorte de service de connexion) et si l'identification par nom d'utilisateur est utilisée, y a t-il une nouvelle association de sécurité négociée qui utilise un certificat à la granularité de l'utilisateur ? Si oui, quand ?

f. Quelle forme d'authentification devrait être utilisée ? Les choix incluent des secrets pré-partagés et des certificats.

g. Comment les participants sont-ils autorisés à effectuer les opérations qu'ils demandent ? Par exemple, tous les appareils avec un certificat provenant d'une source particulière sont ils autorisés à utiliser toute application avec IPsec ou accéder à toutes les ressources ? (Ce problème peut bien sûr apparaître avec tout service de sécurité.)

h. Lesquelles des nombreuses variantes de IKE doivent être prises en charge ? Mode principal ? Mode agressif ?
Noter qu'il y a deux différentes versions de IKE : IKE et IKEv2. IKEv2 est plus simple et plus propre, mais n'est pas encore largement disponible. On doit spécifier quelle version de IKE est exigée.

i. Une prise en charge d'IPsec convenable est elle disponible dans les configurations probables des produits qui vont devoir employer IPsec ?

9. Exemple

Examinons maintenant un exemple fondé sur ces lignes directrices. On va utliser le protocole de routeur fonrtière (BGP, *Border Gateway Protocol*) [RFC4271] pour montrer comment évaluer et spécifier l'utilisation de IPsec pour la sécurité de transmission, plutôt que le mécanisme décrit dans la [RFC2385]. Noter qu'on ne dit pas que IPsec est un choix approprié ici. On démontre plutôt le processus nécessaire d'examen et de spécification. Noter aussi que les problèmes de sécurité plus profonds soulevés par BGP ne sont pas traités par IPsec ni par un autre mécanisme de sécurité de la transmission ; voir [Kent00a] et [Kent00b] pour les détails.

Sélecteurs : BGP fonctionne entre des paires d'hôtes configurés manuellement sur l'accès TCP 179. Le sélecteur approprié serait la paire de locuteurs BGP, pour cet accès seulement. Noter que "l'adresse de rebouclage" du routeur est presque certainement l'adresse d'utilisateur.

Mode : le mode transport serait le choix approprié si IPsec était utilisé. Les informations communiquées ne sont généralement pas confidentielles, de sorte que le chiffrement n'a pas besoin d'être utilisé. AH ou ESP peut être utilisé ; si ESP est utilisé, l'adresse IP de l'envoyeur va devoir être confrontée à l'adresse IP affirmée dans l'échange de gestion de clé. (Cette vérification est rendue obligatoire par la [RFC2401].) Pour l'interopérabilité, AH ou ESP va devoir être spécifié comme de mise en œuvre obligatoire.

Gestion de clé : pour permettre la détection de répétition, un système automatique de gestion de clé devrait être utilisé, probablement IKE. Là encore, l'auteur de RFC devrait en choisir un.

Politique dé sécurité : les connexions devraient être acceptées seulement de l'homologue désigné. (Noter que cette restriction s'applique seulement à BGP. Si le routeur -- ou un hôte IPsec – fait fonctionner plusieurs services avec des besoins de sécurité différents, chacun de ces services exige sa propre politique de sécurité.)

Authentification : étant donné le nombre de routeurs parlant BGP utilisés en interne par les grands FAI, il est probable que les mécanismes de clé partagée ne sont pas adéquats. Par conséquent, IKE fondé sur le certificat doit être pris en charge. Cependant, le mode secret partagé est raisonnable sur les liaisons d'échange de trafic ou (peut-être) sur les liaisons entre FAI et consommateurs. Quel que soit le schéma utilisé, il doit relier à une adresse IP de source ou à un numéro de système autonome (SA, *Autonomous System*) d'une façon ou d'une autre, car d'autres politiques BGP sont exprimées dans ces termes. Si des certificats sont utilisés, vont-ils utiliser des adresses IP ou des numéros d'AS ? Lesquels ?

Disponibilité : pour ce scénario, la disponibilité est la question cruciale. Est ce que les locuteurs BGP probables – routeurs de cœur de réseau et routeurs d'accès -- prennent en charge le profil d'IPsec décrit ci-dessus ? L'utilisation de IPsec, avec ses opérations coûteuses de chiffrement, soulève t-elle un problème de nouvelles attaques de déni de service ? Le groupe de travail et l'IESG doivent déterminer cela avant de décider d'utiliser IPsec pour protéger BGP.

10. Considérations sur la sécurité

IPsec assure seulement la sécurité de transmission et un simple contrôle d'accès. Il y a de nombreuses autres dimensions de la sécurité des protocoles qui sortent du domaine d'application de ce mémoire, incluant en particulier la disponibilité. Par exemple, utiliser IPsec a peu d'effet pour se défendre contre les attaques de déni de service ; dans certaines situations, c'est-à-dire, sur des systèmes à CPU limitée, il peut contribuer à l'attaque. Dans ce domaine, la sécurité de tout protocole résultant dépend largement de la précision de l'analyse qui a résulté en la décision d'utiliser IPsec.

11. Remerciements

Ran Atkinson, Lakshminath Dondeti, Barbara Fraser, Paul Hoffman, Russ Housley, Stephen Kent, Eric Fleischman, membres de l'IESG, et beaucoup d'autres, ont fait de nombreuses suggestions utiles.

12. Références

12.1 Références normatives

[RFC2401] S. Kent et R. Atkinson, "Architecture de sécurité pour le protocole Internet", novembre 1998. (*Obsolète, voir* RFC4301)

[RFC2402] S. Kent et R. Atkinson, "En-tête d'authentification IP", novembre 1998. (*Obsolète, voir* RFC4302, 4305)

[RFC2406] S. Kent et R. Atkinson, "Encapsulation de charge utile de sécurité IP (ESP)", novembre 1998. *(Ob., voir* RFC4303)

[RFC2409] D. Harkins et D. Carrel, "L'échange de clés Internet (IKE)", novembre 1998. *(Obsolète, voir la* RFC4306)

[RFC3554] S. Bellovin et autres, "Utilisation du protocole de transmission de commandes de flux (SCTP) avec IPsec", juillet 2003. *(P.S.)*

[RFC3948] A. Huttunen et autres, "Encapsulation UDP de paquets ESP d'IPsec", janvier 2005. *(P.S.)*

[RFC4107] S. Bellovin, R. Housley, "Lignes directrices pour la gestion des clés de chiffrement", juin 2005, DOI 10.17487/RFC4107, (BCP0107)

[RFC5280] D. Cooper et autres, "Profil de certificat d'infrastructure de clé publique X.509 et de liste de révocation de certificat (CRL) pour l'Internet", mai 2008. (*Remplace les* RFC3280, RFC4325, RFC4630) *(P.S. ; MàJ par* RFC8398, 8399)

[RFC5374] B. Weis et autres, "Extensions de diffusion groupée à l'architecture de sécurité du protocole Internet", novembre 2008. (*P.S.)*

12.2 Références pour information

[Bell96] Bellovin, S., "Problem Areas for the IP Security Protocols", Proc. Sixth Usenix Security Symposium, pp. 205-214, 1996.

[Kent00a] Kent, S., Lynn, C., and K. Seo, "Secure Border Gateway Protocol (Secure-BGP)", IEEE Journal on Selected Areas in Communications, 18:4, pp. 582-592, 2000.

[Kent00b] Kent, S., Lynn, C., Mikkelson, J., and K. Seo, "Secure Border Gateway Protocol (Secure-BGP) -- Real World Performance and Deployment Issues", Proc. Network and Distributed System Security Symposium (NDSS), 2000.

[RFC2385] A. Heffernan, "Protection des sessions de BGP via l'option de signature MD5 de TCP", août 1998. *(P.S.* ; *MàJ par la* RFC6691) *; remplacée par* RFC5925)

[RFC2461] T. Narten, E. Nordmark, W. Simpson, "Découverte de voisins pour IP version 6 (IPv6)", décembre 1998. (*Obsolète, voir* RFC4861) *(D.S.)*

[RFC2661] W. Townsley, A. Valencia, A. Rubens, G. Pall, G. Zorn et B. Palter, "Protocole de tunnelage de couche 2 "L2TP"", *(P.S.)*

[RFC3547] M. Baugher, B. Weis, T. Hardjono et H. Harney, "Le domaine d'interprétation de groupe", juillet 2003. *(Obsolète, voir la* RFC6407)

[RFC3552] E. Rescorla, B. Korver, "Lignes directrices pour la rédaction d'une section de considérations sur la sécurité dans les RFC", juillet 2003. (BCP0072)

[RFC3715] B. Aboba, W. Dixon, "Exigences de compatibilité entre IPsec et la traduction d'adresse réseau (NAT)", mars 2004. *(Info.)*

[RFC3830] J. Arkko et autres, "MIKEY : Gestion de clé multimédia pour l'Internet", août 2004. (*MàJ par* RFC4738) *(P.S.)*

[RFC4271] Y. Rekhter, T. Li et S. Hares, "Protocole de routeur frontière version 4 (BGP-4)", janvier 2006. *(D.S.) (MàJ par* RFC6608, RFC8212, RFC9072)

[RFC4301] S. Kent et K. Seo, "Architecture de sécurité pour le protocole Internet", décembre 2005. *(P.S.) (Remplace la* RFC2401)

[RFC4302] S. Kent, "En-tête d'authentification IP", décembre 2005. *(P.S.)*

[RFC4303] S. Kent, "Encapsulation de charge utile de sécurité dans IP (ESP)", décembre 2005. (*Remplace* RFC2406) *(P.S.)*

[RFC4306] C. Kaufman, "Protocole d'échange de clés sur Internet (IKEv2)", décembre 2005. *(Obsolète, voir la* RFC5996)

[RFC4430] S. Sakane et autres, "Négociation de clés Kerberos sur Internet (KINK)", mars 2006. *(P.S.)*

[RFC4535] H. Harney et autres, "GSAKMP : protocole de gestion de clés d'association de groupe sécurisé", juin 2006. *(P.S.)*

[RFC4960] R. Stewart, éd., "Protocole de transmission de commandes de flux (SCTP)", septembre 2007. (*Remplace* RFC2960, RFC3309 ; *P.S. ; Remplacée par* RFC9260)

Adresse de l'auteur

Steven M. Bellovin
Columbia University
1214 Amsterdam Avenue
MC 0401
New York, NY 10027
US

téléphone : +1 212 939 7149
mél : bellovin@acm.org