Groupe de travail Réseau
Request for Comments : 3756
Catégorie : Information
Traduction Claude Brière de L'Isle

P. Nikander, Ericsson Research Nomadic Lab
J. Kempf, DoCoMo USA Labs
E. Nordmark, Sun Microsystems Laboratories
mai 2004

Modèle de confiance et menaces pour la découverte de voisin IPv6

Résumé
Les normes existantes de l'IETF spécifient que les mécanismes de découverte de voisin (ND, *Neighbor Discovery*) IPv6 et d'autoconfiguration d'adresse peuvent n'être pas protégés par l'en-tête d'authentification (AH, *Authentication Header*) IPsec. Cependant, les spécifications actuelles limitent les solutions de sécurité à des clés manuelles du fait de problèmes pratiques rencontrés par la gestion automatique de clés. Le présent document spécifie trois modèles de confiance différents et expose les menaces qui relèvent de la découverte de voisin IPv6. L'objet de cette discussion est de définir les exigences pour la sécurisation de la découverte de voisin IPv6.

Table des matières

1. Introduction

Les mécanismes de la découverte de voisin (ND, *Neighbor Discovery*) IPv6 de la RFC2461 [2] et d'autoconfiguration d'adresse de la RFC2462 [3] sont utilisés par les nœuds dans un réseau IPv6 pour apprendre la topologie locale, y compris les transpositions d'adresse IP en adresse MAC pour les nœuds locaux, les adresses IP et MAC des routeurs présents dans le réseau local, et les préfixes d'acheminement servis par les routeurs locaux. Les spécifications actuelles suggèrent que AH d'IPsec de la RFC2402 [1] peut être utilisé pour sécuriser les mécanismes, mais elles ne spécifient pas comment. Il apparaît que l'utilisation des mécanismes actuels d'AH est problématique à cause des problèmes de gestion de clés [8].

Pour résoudre le problème, le groupe de travail pour la découverte sûre de voisin (SEND, *Secure Neighbor Discovery*) a été constitué à l'automne 2002. Le but du groupe de travail est de définir un protocole de prise en charge de la découverte de voisin IPv6 sans exiger d'excessif chiffrement manuel.

L'objet du présent document est de définir les types de réseaux dans lesquels les mécanismes sûrs de découverte de voisin IPv6 sont supposés fonctionner, et les menaces que le ou les protocoles de sécurité doivent traiter. Pour réaliser ces objectifs, le présent document définit d'abord trois différents modèles de confiance, correspondant grossièrement aux

intranets d'entreprise sécurisés, aux réseaux d'accès publics sans fil, et aux purs réseaux ad hoc. Après cela, un certain nombre de menaces sont exposées à la lumière de ces modèles de confiance. Le catalogue des menaces vise à être exhaustif, mais il est probable que certaines menaces y manquent quand même. Donc, des idées de nouvelles menaces à prendre en compte sont sollicitées.

1.1 Remarques

Noter que le mandat du groupe de travail SEND limite la portée du groupe aux fonctions de la découverte sûre de voisin. De plus, le mandat mentionne explicitement la configuration zéro comme un but fondamental derrière la découverte de voisin. L'authentification de réseau d'accès et le contrôle d'accès sortent du domaine d'application du présent travail.

Durant les discussions préparatoire à ce document ont été mentionnés les aspects suivants qui peuvent aider à évaluer les solutions éventuelles :

Configuration zéro
Interaction avec les solutions de contrôle d'accès
Adaptabilité
Efficacité

Cependant, les principaux critères d'évaluation sont formés par les modèles de confiance et les listes de menaces. En d'autres termes, les solutions sont principalement évaluées en regardant comment elles réussissent à sécuriser les réseaux contre les menaces identifiées, et seulement ensuite du point de vue de la configuration, du contrôle d'accès, et de l'efficacité.

IMPORTANT. Le présent document expose occasionnellement des propositions de solution, telles que les adresses générées cryptographiquement (CGA, *Cryptographically Generated Addresses*) [7] et les clés fondées sur l'adresse (ABK, *Address Based Key*) [6]. Cependant, de telles discussions n'ont qu'un objet d'illustration. C'est celui de donner au lecteur une idée plus concrète de *certaines* solutions possibles. De telles discussions N'INDIQUENT PAS de préférence pour ces solutions de la part des auteurs ou du groupe de travail.

On devrait noter que le terme "confiance" est utilisé dans le présent document d'une façon assez peu technique. L'interprétation la plus appropriée est de considérer que c'est l'expression d'une croyance organisationnelle ou collective, c'est-à-dire, l'expression de sentiments communément partagés sur le comportement futur des autres parties impliquées. À l'inverse, le terme "relations de confiance" note une relation mutuelle a priori entre les organisations ou parties impliquées où les parties croient que les autres parties vont se comporter correctement même à l'avenir. Une relation de confiance rend possible de configurer les informations d'authentification et d'autorisation entre les parties, alors que l'absence d'une telle relations rend impossible de préconfigurer de telles informations.

2. Travaux antérieurs

Les RFC qui spécifient les protocoles de découverte de voisin IPv6 [2] et d'autoconfiguration d'adresse [3] contiennent l'exposé nécessaire sur la sécurité dans une section "Considérations pour la sécurité". Certaines des menaces identifiées dans le présent document ont été soulevées dans les RFC d'origine. Le remède recommandé était de sécuriser les paquets impliqués avec un en-tête IPsec AH [1]. Cependant, cette recommandation simplifie un peu trop le problème en laissant à des travaux futurs la gestion de clés AH. Par exemple, un hôte qui tente d'obtenir l'accès à un réseau d'accès public peut avoir ou non les associations de sécurité IPsec requises établies avec le réseau. Dans une situation d'itinérance (mais pas nécessairement mobile) où un utilisateur a actuellement l'accès au réseau à travers un fournisseur de service différent de son fournisseur de rattachement, il est peu probable que l'hôte ait été préconfiguré avec la relation de confiance mutuelle appropriée pour le réseau du fournisseur étranger, lui permettant d'authentifier directement le réseau et d'être lui-même authentifié.

À ce jour, toute association de sécurité IPsec entre l'hôte et les routeurs de dernier bond ou d'autres hôtes sur la liaison va avoir besoin d'être préconfigurée de façon complètement manuelle, car les protocoles de découverte de voisin et d'autoconfiguration d'adresse s'occupent dans une certaine mesure de la façon dont un hôte obtient l'accès initial à une liaison. Donc, si une association de sécurité est exigée pour l'accès initial et si l'hôte n'a pas cette association, il n'y a actuellement pas de moyen normalisé par lequel l'hôte puisse se configurer de façon dynamique avec cette association, même si il a le matériel de clé prérequis minimum nécessaire. Cette situation pourrait induire des problèmes d'administration lorsque se produisent des événements tels que le changement de clé.

De plus, la découverte de voisin et l'autoconfiguration d'adresse utilisent quelques adresses de diffusion groupée fixes plus une gamme de 16 millions d'adresses de diffusion groupée de "nœud sollicité". Une application trop simplifiée de SA

préconfigurées exigerait de préconfigurer un nombre ingérable de SA sur chaque hôte et routeur juste au cas où une certaine adresse de diffusion groupée de nœud sollicité serait utilisée. Les SA préconfigurées sont impraticables pour sécuriser une gamme d'adresses potentielles de cette taille.

3. Modèles de confiance

Quand on considère les diverses solutions de sécurité pour la découverte de voisin IPv6 (ND) [2], il est important de se souvenir des modèles de confiance sous-jacents. Les modèles de confiance définis dans cette section seront utilisés plus loin dans ce document, quand on discutera des menaces spécifiques.

Dans ce qui suit, les mécanismes des RFC2461/RFC2462 sont en gros divisés en deux catégories : découverte de voisin (ND) et découverte de routeur (RD). Le premier note des opérations qui n'impliquent pas principalement les routeurs, alors que les opérations de la seconde le font.

Trois différents modèles de confiance sont spécifiés :

1. Un modèle où tous les nœuds authentifiés se font confiance mutuellement pour se comporter correctement à la couche IP et pour ne pas envoyer de message ND ou RD qui contienne de fausses informations. Ce modèle est vu comme représentant une situation où les nœuds sont sous une seule administration et forment un groupe fermé ou semi fermé. Un intranet d'entreprise en est un bon exemple.

2. Un modèle où il y a un routeur en lequel les autres nœuds du réseau ont confiance pour être un routeur légitime qui achemine de bonne foi les paquets entre le réseau local et tout réseau connecté externe. De plus, le routeur est estimé se comporter correctement à la couche IP et ne pas envoyer de message ND ou RD qui contienne de fausses informations.

   Ce modèle est vu comme représentant un réseau public géré par un opérateur. Les clients payent l'opérateur, ont ses accréditifs, et lui font confiance pour fournir le service de transmission IP. Les clients ne se font pas confiance les uns les autres pour se comporter correctement ; tout autre nœud client doit être considéré comme capable d'envoyer des messages ND et RD falsifiés.

3. Un modèle où les nœuds ne se font pas directement confiance l'un l'autre à la couche IP. Ce modèle est considéré comme convenable pour, par exemple, des réseaux ad hoc.

Noter que bien que les nœuds soient supposés se faire confiance les uns les autres dans le premier modèle de confiance (intranet d'entreprise) il est quand même souhaitable de limiter la portée des dommages qu'un nœud est capable d'infliger au réseau local si il se trouve compromis.

3.1 Modèle d'intranet d'entreprise

Dans un intranet d'entreprise ou autre réseau où tous les nœuds sont sous un domaine administratif, les nœuds peuvent être considérés comme fiables à la couche IP. Donc, une fois qu'un nœud a été accepté comme membre du réseau, on suppose qu'il va se comporter de manière fiable.

Sous ce modèle, si le réseau est physiquement sécurisé ou si la couche liaison est sécurisée cryptographiquement dans la mesure nécessaire, aucune autre protection n'est nécessaire pour la ND IPv6, pour autant qu'aucun des nœuds ne devienne compromis. Par exemple, un LAN filaire avec contrôle d'accès 802.1x ou un WLAN avec un réseau à sécurité robuste (RSN, *Robust Security Network*) 802.11i avec chiffrement AES peut être considéré comme assez sûr, n'exigeant pas d'autre protection sous ce modèle de confiance. D'un autre côté, la sécurité de ND ajouterait une profondeur de protection même sous ce modèle (voir plus loin). De plus, on ne devrait pas surestimer le niveau de sécurité que tout mécanisme de couche 2 est capable de procurer.

Si le réseau n'est pas physiquement sécurisé et si la couche liaison n'a pas de protection cryptographique, ou si la protection cryptographique n'est pas assez sûre (par exemple, juste 802.1x et pas 802.11i dans un WLAN) les nœuds dans le réseau peuvent être vulnérables à certaines ou à toutes les menaces mentionnées à la Section 4. Dans un tel cas, une certaine protection est souhaitable pour sécuriser ND. Fournir une telle protection entre dans l'objet initial principal du groupe de travail SEND.

De plus, il est souhaitable de limiter la quantité de dommages potentiels dans le cas où un nœud serait compromis. Par exemple, il peut encore être acceptable qu'un nœud compromis soit capable de lancer une attaque de déni de service mais il n'est pas souhaitable qu'il soit capable de capturer les connexions existantes ou d'établir des attaques par interposition sur de nouvelles connexions.

Comme mentionné à la Section 2, une possibilité pour sécuriser ND serait d'utiliser AH IPsec avec des clé symétriques partagées, connues par tous les nœuds de confiance et par personne à l'extérieur. Cependant, aucun des mécanismes de distribution automatique de clé actuellement normalisé ne fonctionne sans adaptations préalables. Pour plus de détails, voir [8]. De plus, l'utilisation de clé partagées ne protègerait pas contre un nœud compromis.

Plus précisément, le protocole d'accord de clé actuellement utilisé, IKE, souffre d'un problème du type de la poule et de l'œuf [8] : on a besoin d'une adresse IP pour faire fonctionner IKE, IKE est nécessaire pour établir les SA IPsec, et les SA IPsec sont nécessaires pour configurer une adresse IP. De plus, il ne semble pas qu'il y ait de façon rapide et efficace de sécuriser ND avec une cryptographie à clés symétriques. Le nombre d'associations de sécurité requises serait très élevé [9].

À titre d'exemple, une approche possible pour surmonter cette limitation est d'utiliser la cryptographie à clés publiques, et de sécuriser les paquets ND directement avec les signatures de clé publique.

3.2 Réseau public sans fil avec un opérateur

Un scénario où un opérateur gère un réseau public sans fil (ou filaire) par exemple un WLAN dans un hôtel, un aéroport, ou un café, a un modèle de confiance différent. Ici, les nœuds peuvent être supposés faire confiance à l'opérateur pour fournir le service de transmission IP d'une manière digne de confiance, et ne pas interrompre ou envoyer en fausse direction le trafic des clients. Cependant, les clients ne se font généralement pas confiance les uns les autres. Normalement, le ou les routeurs tombent dans un domaine administratif, et les nœuds clients tombent chacun dans leur propre domaine administratif.

On suppose que dans ce scénario, l'opérateur authentifie tous les nœuds clients, ou au moins exige l'autorisation sous forme d'un payement. En même temps, les clients doivent être capables d'authentifier le routeur et s'assurer qu'il appartient à l'opérateur de confiance. Selon le protocole d'authentification de couche liaison et son déploiement, la couche liaison peut prendre soin de l'authentification mutuelle. Le protocole d'authentification de couche liaison peut permettre aux nœuds clients et au routeur d'accès de créer une association de sécurité. Noter qu'il existe des protocoles d'authentification, par exemple, des méthodes EAP particulières, qui ne créent pas de matériel de clé sûr et/ou ne permettent pas au client d'authentifier le réseau.

Dans ce scénario, sécuriser cryptographiquement la couche liaison ne bloque pas nécessairement toutes les menaces évoquées à la Section 4 ; voir les descriptions de menaces individuelles. Précisément, même dans RSN 802.11i avec chiffrement AES, les clés de diffusion et de diffusion groupée sont partagées entre tous les nœuds. Même si la couche de liaison sous-jacente connaît les adresse de couche liaison de tous les nœuds, et est capable de vérifier qu'aucune adresse de source n'a été falsifiée, il y aura quand même des vulnérabilités.

On devrait aussi noter que la sécurité de couche liaison et la topologie IP ne correspondent pas nécessairement. Par exemple, le point d'accès sans fil peut n'être pas visible du tout à la couche IP. Dans un tel cas, la sécurité cryptographique à la couche liaison ne fournit aucune sécurité par rapport à la découverte de voisin IP.

Il semble qu'il y ait au moins deux façons d'assurer la sécurité dans ce scénario. Une possibilité semble être de mettre en place une forte sécurité entre les clients et le routeur d'accès, et de mettre le routeur d'accès au courant des détails du protocole IP et de couche liaison. C'est-à-dire que le routeur va vérifier le contenu des paquets ICMPv6, et filtrer les paquets qui contiennent des informations qui ne correspondent pas à la topologie du réseau. L'autre façon éventuellement acceptable est d'ajouter une protection cryptographique aux paquets ICMPv6 qui portent des messages ND.

3.3 Réseaux ad hoc

Dans un réseau ad hoc, ou dans tout réseau sans opérateur de confiance, aucun des nœuds ne peut se fier aux autres. Dans un cas générique, les nœuds se rencontrent les uns les autres pour la première fois, et il n'y a aucune garantie que les autres nœuds vont se conduire correctement à la couche IP. On doit les considérer comme suspects d'envoyer des messages ND et RD falsifiés.

Comme il n'y a pas de relation de confiance a priori, les nœuds ne peuvent pas s'appuyer sur une authentification traditionnelle. C'est-à-dire que les protocoles d'authentification traditionnels s'appuient sur des relations existantes entre les parties. La relation peut être directe ou indirecte. Le cas indirect s'appuie sur un ou plusieurs tiers de confiance, par lesquels créer une chaîne de relations de confiance entre les parties.

Dans le cas générique de réseau ad hoc, il n'y a pas de tiers de confiance, pas plus que les parties ne se font confiance directement entre elles. Donc, le moyen traditionnel d'authentifier d'abord puis d'autoriser les usagers (à utiliser leurs adresses) ne fonctionne pas.

Il est encore possible d'utiliser des mécanismes d'auto identification,telles que les adresses générées cryptographiquement (CGA, *Cryptographically Generated Addresses*) [7]. Elles permettent aux nœuds de s'assurer qu'ils parlent aux mêmes nœuds (qu'avant) à tout moment, et que chacun des nœuds a bien généré lui-même son adresse IP et n'a pas "volé" l'adresse de quelqu'un d'autre. Il est aussi possible d'apprendre les identités de tout routeur en utilisant diverses sortes d'heuristiques, telles que de vérifier la capacité du nœud à convoyer du trafic protégé cryptographiquement vers un nœud connu et de confiance quelque part dans l'Internet. Des méthodes comme celle là semblent atténuer (mais pas bloquer complètement) certaines des attaques mentionnées dans la section suivante.

4. Menaces sur une liaison (publique) multi-accès

Dans cette section, on expose les menaces contre les mécanismes actuels de découverte de voisin IPv6, quand ils sont utilisés sur des liaisons multi-accès. Les menaces sont exposées à la lumière des modèles de confiance définis à la section précédente.

Il y a trois types généraux de menaces :
1. Des attaques de redirection dans lesquelles un nœud malveillant redirige les paquets loin du routeur de dernier bond ou autre receveur légitime vers un autre nœud sur la liaison.
2. Des attaques de déni de service (DoS, *Denial-of-Service*) dans lesquelles un nœud malveillant empêche la communication entre le nœud attaqué et tous les autres nœuds, ou une adresse de destination spécifique.
3. Des attaques de déni de service (DoS) par inondation, dans lesquelles un nœud malveillant redirige le trafic d'autres hôtes sur un nœud victime, créant par là une inondation de trafic parasite chez l'hôte victime.

Une attaque en redirection peut être utilisée pour des besoins de DoS en faisant que le nœud auquel les paquets ont été redirigés les abandonne, soit complètement soit en transmettant sélectivement certains d'entre eux et pas les autres.

Les paragraphes suivants identifient les menaces spécifiques pour les adresses réseau IPv6. Les descriptions de menaces sont organisées en trois sous-paragraphes. On considère d'abord les menaces qui n'impliquent pas les routeurs ou les informations d'acheminement. On considère ensuite les menaces qui impliquent les routeurs ou les informations d'acheminement. Enfin, on considère les attaques en répétition et les menaces qui sont exploitables à distance. Toutes les menaces sont exposées à la lumière des modèles de confiance.

4.1 Menaces qui ne sont pas en relation avec le routeur ou l'acheminement

Dans cette section, on expose les attaques contre les "pures" fonctions de découverte de voisin, c'est-à-dire, la découverte de voisin (ND, *Neighbor Discovery*), la détection d'inaccessibilité du voisin (NUD, *Neighbor Unreachability Detection*), et la détection d'adresse dupliquée (DAD, *Duplicate Address Detection*) dans l'autoconfiguration d'adresse.

4.1.1 Usurpation de sollicitation/annonce de voisin

Les nœuds sur la liaison utilisent les messages Sollicitation de voisin et Annonce de voisin pour créer des liens entre les adresses IP et les adresses MAC. Plus précisément, il y a deux cas lorsque un nœud crée des entrées d'antémémoire de voisin à réception des sollicitations :
1. Un nœud reçoit une Sollicitation de voisin qui contient une adresse de nœud. Le nœud peut utiliser cela pour remplir son antémémoire de voisin. C'est fondamentalement une optimisation de performances, et un DEVRAIT dans les documents de base.
2. Durant une détection d'adresse dupliquée (DAD), si un nœud reçoit une Sollicitation de voisin pour la même adresse qu'il sollicite, la situation est considérée comme une collision, et le nœud doit cesser de solliciter pour ladite adresse.

À l'opposé des messages de sollicitation qui créent ou modifient l'état seulement dans ces occasions spécifiques, l'état est usuellement modifié chaque fois qu'un nœud reçoit un message d'annonce pour lequel il a sollicité.

Un nœud attaquant peut provoquer l'envoi de paquets pour des nœuds légitimes, aussi bien des hôtes que des routeurs, à une autre adresse de couche liaison. Cela peut être fait soit en envoyant une Sollicitation de voisin avec une option d'adresse de couche liaison de source différente, soit en envoyant une Annonce de voisin avec une option d'adresse de couche liaison de cible différente.

Les attaques réussissent parce que l'entrée d'antémémoire de voisin avec la nouvelle adresse de couche liaison se substitue à l'ancienne. Si l'adresse de couche liaison usurpée est une adresse valide, tant que l'attaquant répond aux messages Sollicitation de voisin en envoi individuel envoyés au titre de la détection d'inaccessibilité de voisin, les paquets vont

continuer d'être redirigés. C'est une attaque de redirection/DoS.

Ce mécanisme peut être utilisé pour une attaque de DoS en spécifiant une adresse de couche liaison non utilisée ; cependant, cette attaque de DoS sera d'une durée limitée car après 30 à 50 secondes (avec des valeurs de temporisateur par défaut) le mécanisme de détection d'inaccessibilité de voisin va éliminer la mauvaise adresse de couche liaison et envoyer une nouvelle diffusion groupée pour découvrir l'adresse de couche liaison. Par conséquent, l'attaquant devra continuer de répondre avec des adresses de couche liaison fabriquées si il veut maintenir l'attaque au delà de la fin de temporisation.

La menace exposée dans ce paragraphe implique les messages Sollicitation de voisin et Annonce de voisin.

Cette attaque ne pose pas de problème si l'accès à la liaison est restreint aux nœuds de confiance ; si un nœud de confiance est compromis, les autres nœuds sont exposés à cette menace. Dans le cas où seul l'opérateur est de confiance, les nœuds peuvent s'appuyer sur l'opérateur pour certifier les liens d'adresse pour les autres nœuds locaux. Du point de vue de la sécurité, le routeur peut agir comme un mandataire de confiance pour les autres nœuds. Cela suppose que le routeur puisse être de confiance pour représenter correctement les autres nœuds de la liaison. Dans le cas du réseau ad hoc, et facultativement dans les deux autres cas, les nœuds peuvent utiliser les techniques d'auto certification (par exemple, CGA) pour autoriser les liens d'adresses.

De plus, certaines mises en œuvre enregistrent une erreur et refusent d'accepter les recouvrements de ND, exigeant à la place que l'ancienne entrée arrive d'abord en fin de temporisation.

4.1.2 Échec de détection d'inaccessibilité de voisin (NUD)

Les nœuds sur la liaison surveillent l'accessibilité des destinations locales et des routeurs avec la procédure de détection d'inaccessibilité de voisin [2]. Normalement, les nœuds s'appuient sur les informations de couche supérieure pour déterminer si les nœuds homologues sont encore accessibles. Cependant, si il y a un délai suffisamment long sur le trafic de couche supérieure, ou si le nœud arrête de recevoir des réponses d'un nœud homologue, la procédure de NUD est invoquée. Le nœud envoie un NS ciblé au nœud homologue. Si l'homologue est encore accessible, il va répondre par un NA. Cependant, si le nœud solliciteur ne reçoit pas de réponse, il essayera encore quelques fois, et finira par supprimer l'entrée de l'antémémoire de voisin. Si nécessaire, cela déclanche le protocole standard de résolution d'adresse pour apprendre la nouvelle adresse MAC. Aucun trafic de niveau supérieur ne peut se poursuivre si cette procédure purge les entrées d'antémémoire de voisin après avoir déterminé (peut-être à tort) que l'homologue n'est pas joignable.

Un nœud malveillant peut continuer d'envoyer des NA fabriqués en réponse à des messages NS NUD. Sauf si les messages NA sont par ailleurs protégés, l'attaquant peut être capable d'étendre l'attaque pendant longtemps en utilisant cette technique. Les conséquences réelles dépendent de pourquoi le nœud est devenu inaccessible pour la première fois, et de comment le nœud cible va se comporter si il sait que le nœud est devenu injoignable. C'est une attaque de DoS.

La menace exposée dans ce paragraphe implique des messages Sollicitation/Annonce de voisin.

Cette attaque n'est pas un problème si l'accès à la liaison est restreint aux nœuds de confiance ; si un nœud de confiance est compromis, les autres nœuds sont exposés à cette attaque de DoS. Da,s les deux autres modèles de confiance, une solution exige que le nœud qui effectue la NUD soit capable de faire la distinction entre des réponses NA authentiques et fabriquées.

4.1.3 Attaque de DoS sur la détection d'adresse dupliquée

Dans les réseaux où les hôtes entrants obtiennent leurs adresses en utilisant l'autoconfiguration d'adresse sans état [3], un nœud attaquant pourrait lancer une attaque de DoS en répondant à toute tentative de détection d'adresse dupliquée faite par un hôte entrant. Si l'attaquant revendique l'adresse, l'hôte ne sera jamais capable d'obtenir une adresse. L'attaquant peut revendiquer l'adresse de deux façons : il peut répondre par un NS, faisant semblant d'effectuer aussi la DAD, ou il peut répondre par un NA, faisant semblant d'avoir déjà pris l'adresse pour l'utiliser. Cette menace a été identifiée dans la RFC2462 [3]. Le problème peut aussi se présenter lorsque d'autres types de configuration d'adresse sont utilisés, c'est-à-dire, chaque fois que la DAD est invoquée avant de réellement configurer l'adresse suggérée. C'est une attaque de DoS.

La menace exposée dans ce paragraphe implique des messages Sollicitation/Annonce de voisin.

Cette attaque ne pose pas de problème si l'accès à la liaison est restreint aux nœuds de confiance ; si un nœud de confiance est compromis, les autres nœuds deviennent exposés à cette menace de DoS. Dans les deux autres modèles de confiance, une solution exige que le nœud qui effectue la DAD soit capable de vérifier si l'envoyeur de la réponse NA est autorisé à utiliser ou non cette adresse IP. Dans le cas de l'opérateur de confiance, l'opérateur peut agir comme un donneur

d'autorisations, gardant trace des adresses allouées et s'assurant qu'aucun nœud n'a plus de quelques (centaines de) adresses allouées. D'un autre côté, il peut être dommageable d'adopter une telle pratique, car il peut y avoir des situations où il est souhaitable pour un nœud d'avoir un grand nombre d'adresses, par exemple, pour créer une adresse séparée par connexion TCP, ou lorsque on fonctionne avec un mandataire ND. Donc, il peut être inapproprié de suggérer que les FAI pourraient exercer un contrôle sur le nombre d'adresses qu'un hôte légitime peut avoir ; la discussion ci-dessus ne doit être considérée que comme un exemple, comme on l'a dit au début de ce document.

Dans le cas de réseau ad hoc, on peut vouloir structurer les adresses de telle façon que l'auto autorisation soit possible.

4.2 Menaces impliquant le routeur/acheminement

Dans cette section, on considère les menaces qui relèvent de la découverte de routeur ou autre mécanisme avec l'assistance du routeur ou en relation avec le routeur.

4.2.1 Routeur de dernier bond malveillant

Cette menace a été identifiée dans [5] mais a été classée comme menace générale sur IPv6 et non spécifique de IPv6 mobile. Elle est aussi identifiée dans la RFC2461 [2]. Cette menace est une attaque de redirection/DoS.

Un nœud attaquant sur le même sous-réseau qu'un hôte tentant de découvrir un router de dernier bond légitime pourrait se faire passer pour un routeur de dernier bond IPv6 en envoyant en diffusion groupée des annonces de routeur IPv6 ou des annonces de routeur en envoi individuel qui paraissent légitimes en réponse à des sollicitations d'annonce de routeur en diffusion groupée provenant d'un hôte entrant. Si l'hôte entrant choisit l'attaquant comme son routeur par défaut, l'attaquant a l'opportunité de siphonner le trafic provenant de l'hôte, ou de monter une attaque par interposition. L'attaquant pourrait s'assurer que l'hôte entrant le choisit comme routeur par défaut en envoyant en diffusion groupée des annonces de routeur périodiques pour le routeur de dernier bond réel avec une durée de vie de zéro. Cela peut mystifier l'hôte entrant en lui faisant croire que le routeur d'accès réel ne veut pas prendre de trafic. Une fois accepté comme un routeur légitime, l'attaquant pourrait envoyer des messages Redirection aux hôtes, puis disparaître, effaçant ainsi ses traces.

Cette menace est partiellement atténuée dans la RFC2462 ; au paragraphe 5.5.3 de la RFC2462 il est exigé que si la durée de vie du préfixe annoncé est inférieure à 2 heures et inférieure à la durée de vie mémorisée, la durée de vie mémorisée n'est pas réduite sauf si le paquet a été authentifié. Cependant, la procédure de choix du routeur par défaut, telle que définie au paragraphe 6.3.6 de la RFC2461, ne contient pas une telle règle.

La menace exposée dans ce paragraphe implique les messages Annonce de routeur et Sollicitation d'annonce de routeur.

Cette attaque ne pose pas de problème si l'accès est restreint aux nœuds de confiance ; si un nœud de confiance est compromis, les autres nœuds sont exposés à cette menace. Cependant, la menace peut être partiellement atténuée par un certain nombre de moyens, par exemple, en configurant les nœuds à préférer les routeurs existants aux nouveaux. Noter que cette approche n'empêche pas nécessairement d'introduire de nouveaux routeurs dans le réseau, selon les détails de mise en œuvre. Au minimum, elle fait que les nœuds existants préfèrent les routeurs existants aux nouveaux.

Dans le cas d'un opérateur de confiance, il doit y avoir un moyen pour que les nœuds fassent la distinction entre les routeurs dignes de confiance, gérés par l'opérateur, et les autres nœuds. Il n'y a pas actuellement de solutions largement acceptées pour le cas du réseau ad hoc, et le problème reste l'objet de recherches.

4.2.2 Mort du routeur par défaut

Dans cette attaque, un attaquant 'tue' le ou les routeurs par défaut, amenant par là les nœuds sur la liaison à supposer que tous les nœuds sont locaux. Au paragraphe 5.2 de la RFC2461 [2] il est indiqué que "[si] la liste de routeurs par défaut est vide, l'envoyeur suppose que la destination est en-liaison". Donc, si l'attaquant est capable de faire croire à un nœud qu'il n'y a pas de routeur par défaut sur la liaison, le nœud va essayer d'envoyer les paquets directement, en utilisant la découverte de voisin. Après cela, l'attaquant peut utiliser la mystification NS/NA même contre des destinations hors liaison.

On a identifié quelques unes des façons dont un attaquant peut 'tuer' le ou les routeurs par défaut. L'une d'elles est de lancer une attaque de DoS classique contre le routeur afin qu'il n'apparaisse plus comme répondant aux sollicitations. L'autre est d'envoyer une annonce de routeur falsifiée avec une durée de vie de routeur de zéro (voir le paragraphe 6.3.4 de la RFC 2461 [2]). Cependant, voir aussi la discussion du paragraphe 4.2.1 ci-dessus.

Cette attaque est principalement une attaque de DoS, mais elle pourrait aussi être utilisée pour rediriger le trafic vers le meilleur routeur suivant, qui peut être l'attaquant.

La menace exposée dans ce paragraphe implique les messages Annonce de routeur. Une variante de cette menace est possible en surchargeant le routeur, sans utiliser de message ND/RD.

Cette attaque n'est pas un problème si l'accès à la liaison est restreint aux nœuds de confiance ; si un nœud de confiance est compromis, les autres nœuds sont exposés à cette menace. Dans le cas d'un opérateur de confiance, il doit y avoir un moyen pour que les nœuds fassent la distinction entre les routeurs dignes de confiance, gérés par l'opérateur, et les autres nœuds. Cela protège contre les annonces de routeur falsifiées, mais cela ne protège pas contre la surcharge du routeur. Il n'y a actuellement pas de solution largement acceptée pour le cas du réseau ad hoc, et la question reste un objet de recherches.

Merci à Alain Durand (AFNOR) pour avoir identifié cette menace.

4.2.3 Le bon routeur va mal

Dans cette attaque, un routeur qui était auparavant de confiance se trouve compromis. Les attaques disponibles sont les mêmes que celles discutées au paragraphe 4.2.1. C'est une attaque de redirection/DoS.

Il n'y a actuellement pas de solution connue pour les trois modèles de confiance présentés. D'un autre côté, sur une liaison multi-routeur, on peut imaginer une solution impliquant la révocation des droits du routeur. La situation reste l'objet de recherches.

4.2.4 Message Redirection falsifié

Le message Redirection peut être utilisé pour envoyer des paquets pour une certaine destination à toute adresse de couche liaison sur la liaison. L'attaquant utilise l'adresse de liaison locale du routeur de premier bond actuel afin d'envoyer un message Redirection à un hôte légitime. Comme l'hôte identifie le message par l'adresse de liaison locale comme venant de son routeur de premier bond, il accepte la redirection. Tant que l'attaquant répond aux sondes de détection d'inaccessibilité de voisin à l'adresse de couche liaison, la redirection va rester efficace. C'est une attaque de redirection/DoS.

La menace discutée dans ce paragraphe implique les messages Redirection.

Cette attaque n'est pas un problème si l'accès à la liaison est restreint aux nœuds de confiance ; si un nœud de confiance est compromis, les autres nœuds sont exposés à cette menace. Dans le cas d'un opérateur de confiance, il doit y avoir un moyen pour que les nœuds fassent la distinction entre les routeurs dignes de confiance, gérés par l'opérateur, et les autres nœuds. Il n'y a actuellement pas de solution largement acceptée pour le cas du réseau ad hoc, et la question reste un objet de recherches.

4.2.5 Préfixe en liaison bogué

Un nœud attaquant peut envoyer un message Annonce de routeur qui spécifie qu'un certain préfixe de longueur arbitraire est en-liaison. Si un hôte envoyeur pense que le préfixe est en-liaison, il ne va jamais envoyer au routeur un paquet pour ce préfixe. Au lieu de cela, l'hôte va essayer d'effectuer la résolution d'adresse en envoyant des sollicitations de voisin, mais ces sollicitations de voisin ne vont jamais donner de réponse, déniant le service à l'hôte attaqué. C'est une attaque de DoS.

L'attaquant peut utiliser une durée de vie arbitraire dans l'annonce de préfixe bogué. Si la durée de vie est infinie, l'hôte d'envoi va se voir refuser le service jusqu'à ce qu'il perde l'état dans sa liste de préfixes, par exemple, en réamorçant, ou quand ce même préfixe est annoncé avec une durée de vie de zéro. L'attaque pourrait aussi être perpétrée de façon sélective pour les paquets destinés à un préfixe particulier en utilisant des préfixes de 128 bits, c'est-à-dire, des adresses complètes.

De plus, l'attaque peut causer un déni de service par l'inondation du tableau d'acheminement du nœud. Le nœud ne serait plus capable de différencier les préfixes légitimement en-liaison des préfixes bogués lorsque il prend ses décisions sur ceux à garder et ceux à abandonner. Par nature, tout système fini doit avoir des points où les nouveaux préfixes reçus doivent être abandonnés plutôt qu'acceptés

Cette attaque peut être étendue en une attaque de redirection si l'attaquant répond aux sollicitations de voisin par des annonces de voisin mystificatrices, trompant ainsi les nœuds de la liaison pour qu'ils envoient leur trafic, à lui ou à quelque autre nœud.

Cette menace implique le message Annonce de routeur. L'attaque étendue combine l'attaque définie au paragraphe 4.1.1 et dans ce paragraphe, et implique les messages Sollicitation de voisin, Annonce de voisin et Annonce de routeur.

Cette attaque n'est pas un problème si l'accès à la liaison est restreint aux nœuds de confiance ; si un nœud de confiance est compromis, les autres nœuds sont exposés à cette menace. Dans le cas d'un opérateur de confiance, il doit y avoir un moyen pour que les nœuds fasse la distinction entre les routeurs dignes de confiance, gérés par l'opérateur, et les autres nœuds. Il n'y a actuellement pas de solution largement acceptée pour le cas du réseau ad hoc, et la question reste un objet de recherches.

À titre d'exemple, une approche possible pour limiter les dommages de cette attaque est d'exiger que les préfixes annoncés comme en-liaison soient /64s (autrement, il est facile d'annoncer quelque chose de court comme 0/0 et cette attaque est très facile).

4.2.6 Préfixe de configuration d'adresse bogué

Un nœud attaquant peut envoyer un message Annonce de routeur qui spécifie un préfixe de sous-réseau invalide à utiliser par un hôte pour l'autoconfiguration d'adresse. L'hôte qui exécute l'algorithme d'autoconfiguration d'adresse utilise le préfixe annoncé pour construire une adresse [3], même si cette adresse n'est pas valide pour ce sous-réseau. Il en résulte que les paquets retournés n'atteignent jamais l'hôte parce que l'adresse de source de l'hôte est invalide. C'est une attaque de DoS.

Cette attaque a un potentiel de propagation au delà de l'hôte immédiatement attaqué si celui-ci effectue une mise à jour dynamique sur le DNS sur la base de l'adresse dont la construction est boguée. Les mises à jour du DNS [4] causent l'ajout de l'adresse boguée à l'enregistrement d'adresse de l'hôte dans le DNS. Si cela devait arriver, les applications qui effectuent la résolution de nom par le DNS vont obtenir l'adresse boguée et les tentatives de contacter l'hôte vont échouer. Cependant, les applications bien conçues vont se récupérer et essayer les autres adresses enregistrées dans le DNS, qui peuvent être correctes.

Une attaque répartie peut avoir des conséquences plus sévères en créant une entrée de DNS inverse falsifiée qui corresponde à l'entrée de DNS créée de façon dynamique par la cible. Considérons un attaquant qui a un accès légitime à un préfixe <ATTACK_PRFX>, et une cible qui a un identifiant d'interface <TARGET_IID>. L'attaquant crée une entrée de DNS inverse pour <ATTACK_PRFX>:<TARGET_IID>, pointant sur le nom de domaine réel de la cible, par exemple, "secure.target.com". Ensuite, l'attaquant annonce le préfixe <ATTACK_PRFX> à la liaison de la cible. La cible va créer une adresse <ATTACK_PRFX>:<TARGET_IID>, et mettre à jour son entrée de DNS de telle sorte que "secure.target.com" pointe sur <ATTACK_PRFX>:<TARGET_IID>.

À ce moment, "secure.target.com" pointe sur <ATTACK_PRFX>:<TARGET_IID>, et <ATTACK_PRFX>:<TARGET_IID> pointe sur "secure.target.com". Cette menace est atténuée par le fait que l'attaquant peut être retracé car le propriétaire de <ATTACK_PRFX> est disponible chez les registraires.

Il y a aussi une possibilité d'annonce d'un préfixe de cible comme un préfixe d'autoconfiguration sur une liaison active, en ensuite d'avoir tous les nœuds de cette liaison qui essayent de communiquer avec le monde extérieur avec cette adresse. Si le routeur local n'a pas un filtre d'entrée, la liaison cible peut alors obtenir un grand nombre de réponses pour ces tentatives de communication initiale.

Les menaces de base exposées dans ce paragraphe impliquent les messages Annonce de routeur. Les scénarios d'attaque étendue impliquent aussi le DNS.

Cette attaque n'est pas un problème si l'accès à la liaison est restreint aux nœuds de confiance ; si un nœud de confiance est compromis, les autres nœuds sont exposés à cette menace. Dans le cas d'un opérateur de confiance, il doit y avoir un moyen pour que les nœuds fassent la distinction entre les routeurs dignes de confiance, gérés par l'opérateur, et les autres nœuds. Il n'y a actuellement pas de solution largement acceptée pour le cas du réseau ad hoc, et la question reste un objet de recherches.

4.2.7 Falsification de paramètre

Les annonces de routeur IPv6 contiennent quelques paramètres utilisés pas les hôtes lorsque ils envoient des paquets et pour dire aux hôtes si ils devraient effectuer ou non la configuration d'adresse à états pleins [2]. Un nœud attaquant pourrait envoyer une annonce de routeur paraissant valide qui duplique l'annonce de routeur provenant du routeur par défaut légitime, excepté que les paramètres inclus sont conçus pour perturber le trafic légitime. C'est une attaque de DoS.

Les attaques spécifiques incluent :

1. L'attaquant inclut une limite de bonds actuels de un ou d'un autre petit nombre dont l'attaquant sait qu'il va causer l'abandon des paquets légitimes avant qu'ils n'atteignent leur destination.
2. L'attaquant met en œuvre un serveur ou relais DHCPv6 bogué et le fanion 'M' et/ou 'O' est établi, indiquant que la configuration d'adresse à états pleins et/ou la configuration à états pleins d'autres paramètres devrait être faite. L'attaquant est alors en position de répondre aux interrogations de configuration à état plein d'un hôte légitime avec ses propres réponses bogjuées.

La menace exposée dans ce paragraphe implique les messages Annonce de routeur.

Noter que sécuriser le seul DHCP ne résout pas ce problème. Il y a deux raisons à cela. D'abord, l'attaquant peut empêcher le nœud d'utiliser DHCP en premier lieu. Ensuite, selon la configuration locale du nœud, l'attaquant peut mystifier le nœud pour lui faire utiliser un serveur DHCP qui soit moins de confiance. (Cette dernière est une variante de l'attaque dite "en dégradation".)

À titre d'exemple, une approche possible pour atténuer cette menace est d'ignorer les très petites limites de bond. Les nœuds pourraient mettre en œuvre une limite de bond configurable minimum, et ignorer les tentatives de la régler en dessous de ladite limite.

Cette attaque n'est pas un problème si l'accès à la liaison est restreint aux nœuds de confiance ; si un nœud de confiance est compromis, les autres nœuds sont exposés à cette menace. Dans le cas d'un opérateur de confiance, il doit y avoir un moyen pour que les nœuds fassent la distinction entre les routeurs dignes de confiance, gérés par l'opérateur, et les autres nœuds. Il n'y a actuellement pas de solution largement acceptée pour le cas du réseau ad hoc, et la question reste un objet de recherches.

4.3 Attaques en répétition et attaques exploitables à distance

4.3.1 Attaques en répétition

Tous les messages de découverte de voisin et de découverte de routeur sont enclines aux attaques en répétition. C'est à dire que même si elles étaient cryptographiquement protégées de sorte que leur contenu ne puisse être falsifié, un attaquant serait capable de capturer des messages valides et de les répéter plus tard. Donc, indépendamment du mécanisme choisi pour sécuriser les messages, ce mécanisme doit être protégé contre les attaques en répétition.

Heureusement, il est très facile de déjouer la plupart des attaques en répétition. Dans les échanges demande-réponse, comme les sollicitations-annonces, la demande peut contenir un nom occasionnel qui doit apparaître aussi dans la réponse. Donc, les vieilles réponses ne sont pas valides car elles ne contiennent pas le bon nom occasionnel. De la même façon, les messages autonomes, tels que les messages d'annonce non sollicitée ou de redirection, peuvent être protégés par des horodatages ou des compteurs. En pratique, des horloges et des horodatages à peu près synchronisés semblent bien fonctionner, car les receveurs peuvent garder trace de la différence entre les horloges des différents nœuds, et s'assurer que tout nouveau message est plus récent que le dernier message vu.

4.3.2 Attaques de DoS contre la découverte de voisins

Dans cette attaque, le nœud attaquant commence par fabriquer des adresses avec le préfixe de sous-réseau et leur envoie en continu des paquets. Le routeur de dernier bond est obligé de résoudre ces adresses en envoyant des paquets de sollicitation de voisin. Un nœud légitime qui tente d'entrer sur le réseau peut n'être pas capable d'obtenir le service de découverte de voisin de la part du serveur de dernier bond car celui-ci sera toujours occupé à envoyer d'autres sollicitations. Cette attaque de DoS est différente des autres en ce que l'attaquant peut être hors-liaison. La ressource attaquée dans ce cas est l'antémémoire conceptuelle de voisin, qui sera remplie de tentatives de résolution d'adresses IPv6 qui ont un préfixe valide mais un suffixe invalide. C'est une attaque de DoS.

La menace exposée dans ce paragraphe implique les messages Sollicitation de voisin.

Cette attaque n'implique pas directement les modèles de confiance présentés. Cependant, si l'accès à la liaison est restreint aux nœuds enregistrés, et si le routeur d'accès garde trace des nœuds qui se sont enregistrés pour accéder à la liaison, l'attaque peut être contrée de façon triviale. Cependant, aucun mécanisme de cette sorte n'est actuellement normalisé.

Dans un sens, ce problème est très similaire à celui de l'inondation de SYN TCP. Par exemple, la limitation des sollicitations de voisin, restreignant la quantité d'état réservée pour les sollicitations non résolues, et une gestion habile de l'antémémoire peuvent être appliquées.

On devrait noter que les hôtes et les routeurs doivent tous deux se préoccuper de ce problème. Le cas du routeur a été discuté ci-dessus. Les hôtes sont aussi vulnérables car le processus de découverte de voisin peut éventuellement être abusé par une application qui est arrangée pour envoyer des paquets à des destinations en-liaison arbitraires.

4.4 Résumé des attaques

Colonnes :
N/R : Attaques de découverte de voisin (ND) ou de découverte de routeur (RD)
R/D : Attaques de redirection/DoS (Redir) ou juste de DoS
Msgs : Messages impliqués dans l'attaque : NA, NS, RA, RS, Redir
1 : Présent dans le modèle de confiance 1 (intranet d'entreprise)
2 : Présent dans le modèle de confiance 2 (réseau géré par un opérateur public)
3 : Présent dans le modèle de confiance 3 (réseau ad hoc)

Symboles dans les colonnes de modèle de confiance :
- La menace n'est pas présente ou n'est pas un problème.
+ La menace est présente et il y a au moins une solution connue.
R La menace est présente mais sa solution fait encore l'objet de recherches.

Noter que le signe plus '+' dans le tableau ne signifie pas qu'il y a une solution normalisée prête à l'emploi. Si des solutions existaient, ce document ne serait pas nécessaire. Il note plutôt que dans l'opinion des auteurs le problème a été résolu en principe, et qu'il existe une publication qui décrit une approche pour résoudre le problème, ou qu'une solution peut être produite par application directe de recherches connues et/ou de résultats d'ingénierie.

D'un autre côté, un 'R' indique que les auteurs ne connaissent aucune publication décrivant une solution au problème, et qu'on ne peut envisager au moment de la rédaction d'extension simple et facile de recherches connues et/ou de résultat d'ingénierie pour résoudre le problème.

Paragraphe	Nom de l'attaque	N/R	R/D	Msgs	1	2	3	Notes
4.1.1	Mystification NS/NA	ND	Redir	NA NS	+	+	+	
4.1.2	Défaillance de NUD failure	ND	DoS	NA NS	-	+	+	
4.1.3	DAD DoS	ND	DoS	NA NS	-	+	+	
4.2.1	Routeur malveillant	RD	Redir	RA RS	+	+	R	
4.2.2	Routeur par défaut tué	RD	Redir	RA	+/R	+/R	R	1)
4.2.3	Un bon routeur tourne mal	RD	Redir	RA RS	R	R	R	
4.2.4	Redirection falsifié	RD	Redir	Redir	+	+	R	
4.2.5	Préfixe en-liaison bogué	RD	DoS	RA	-	+	R	2)
4.2.6	Configuration d'adresse bogué	RD	DoS	RA	-	+	R	3)
4.2.7	Paramètre falsifié	RD	DoS	RA	-	+	R	
4.3.1	Attaques en répétition	Tous	Redir	Tous	+	+	+	
4.3.2	DoS contre ND à distance	ND	DoS	NS	+	+	+	

Figure 1

Notes
1. Il est possible de protéger les annonces de routeur, fermant par là une variante de cette attaque. Cependant, fermer l'autre variante (surcharge du routeur) ne semble pas plausible selon le mandat du groupe de travail.
2. Noter que l'attaque étendue définie au paragraphe 4.2.5 combine l'envoi d'un préfixe en-liaison bogué et d'effectuer une mystification de NS/NA selon le paragraphe 4.1.1. Donc, si l'échange NA/NS est sûr, la capacité d'utiliser le paragraphe 4.2.5 pour des redirections est très probablement bloquée aussi.
3. L'enregistrement bogué du DNS résultant d'un enregistrement aveugle de la nouvelle adresse via la mise à jour du DNS [4] n'est pas considéré ici comme un problème de sécurité de ND. Cependant, on devrait le noter comme une possible vulnérabilité dans les mises en œuvre.

Pour une approche légèrement différente, voir aussi la Section 7 de [9]. En particulier le tableau du paragraphe 7.7 de [9] qui est très bon.

5. Considérations pour la sécurité

Le présent document expose les menaces contre la sécurité sur l'accès au réseau dans IPv6. À ce titre, il concerne entièrement la sécurité.

6. Remerciements

Merci à Alper Yegin de DoCoMo Communications Laboratories USA pour l'identification de l'attaque de déni de service de découverte de voisin. Nous tenons aussi à remercier Tuomas Aura et Michael Roe de Microsoft Research Cambridge ainsi que Jari Arkko et Vesa-Matti Mantyla de Ericsson Research Nomadiclab pour les discussions avec nous sur certaines des menaces.

Merci à Alper Yegin, Pekka Savola, Bill Sommerfeld, Vijay Devaparalli, Dave Thaler, et Alain Durand pour leurs commentaires constructifs.

Merci à Craig Metz pour ses nombreux excellents commentaires, et en particulier pour le matériau des mises en œuvre qui refusent d'accepter les débordements de découverte de voisin, pour la menace du préfixe bogué en liaison, et pour nous avoir rappelé les attaques en répétition.

7. Références pour information

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

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

[3] S. Thomson, T. Narten, "Autoconfiguration d'adresse IPv6 sans état", RFC2462, décembre 1998. (*Obsolète, voir* RFC4862) *(D.S.)*

[4] B. Wellington, "Mise à jour dynamique sécurisée du système des noms de domaine (DNS)", RFC3007, novembre 2000.

[5] Mankin, A., "Threat Models introduced by Mobile IPv6 and Requirements for Security in Mobile IPv6", *Non publiée*.

[6] Kempf, J., Gentry, C. and A. Silverberg, "Securing IPv6 Neighbor Discovery Using Address Based Keys (ABKs)", juin 2002. *Non publiée*.

[7] Roe, M., "Authentication of Mobile IPv6 Binding Updates and Acknowledgments", mars 2002. *Non publiée*.

[8] Arkko, J., "Effects of ICMPv6 on IKE", mars 2003. *Non publiée*.

[9] Arkko, J., "Manual Configuration of Security Associations for IPv6 Neighbor Discovery", mars 2003. *Non publiée*.

Adresse des auteurs

Pekka Nikander (éditeur)
Ericsson Research Nomadic Lab
JORVAS FIN-02420
FINLAND
téléphone : +358 9 299 1
mél : pekka.nikander@nomadiclab.com

James Kempf
DoCoMo USA Labs
181 Metro Drive, Suite 300
San Jose, CA 95110
USA
téléphone : +1 408 451 4711
mél : kempf@docomolabs-usa.com

Erik Nordmark
Sun Microsystems
17 Network Circle
Menlo Park, CA 94043
USA
téléphone : +1 650 786 2921
mél : erik.nordmark@sun.com

Déclaration complète de droits de reproduction

Remerciement

Le financement de la fonction d'édition des RFC est actuellement fourni par l'Internet Society.