Groupe de travail Réseau
Request for Comments : 4449
Catégorie : Sur la voie de la normalisation
Traduction Claude Brière de L'Isle

C. Perkins, Nokia Research Center

juin 2006

Sécurisation de l'optimisation de chemin IPv6 mobile avec une clé partagée statique

Résumé
Un nœud mobile et un nœud correspondant peuvent pré configurer des données utiles pour pré calculer une clé de gestion de lien qui puisse être ultérieurement utilisée pour autoriser des mises à jour de liens.

Table des matières

1. Introduction

La présente spécification introduit un mécanisme de sécurité de remplacement à faible latence pour protéger la signalisation relative à l'optimisation de chemin dans IPv6 mobile. Le mécanisme par défaut spécifié dans la [RFC3775] utilise un essai périodique d'acheminement de retour pour vérifier à la fois le "droit" du nœud mobile à utiliser une adresse de rattachement spécifique, ainsi que la validité de l'adresse d'entretien revendiquée. Ce mécanisme n'exige pas de configuration ni d'entités de confiance en dehors de l'agent de rattachement du nœud mobile.

Le mécanisme spécifié dans le présent document, exige cependant la configuration d'un secret partagé entre le nœud mobile et son nœud correspondant. Par suite, les messages relatifs aux essais d'acheminement peuvent être omis, ce qui réduit significativement la latence. De plus, le droit d'utiliser une adresse de rattachement spécifique est assuré d'une manière plus forte que dans la [RFC3775]. Par ailleurs, l'applicabilité de ce mécanisme est limitée par le besoin d'une pré configuration. Ce mécanisme est aussi limité aux seuls scénarios où on peut faire confiance aux nœuds mobiles, car la validité des adresses d'entretien revendiquées n'est pas vérifiée.

Les mots clés "DOIT", "NE DOIT PAS", "EXIGE", "DEVRA", "NE DEVRA PAS", "DEVRAIT", "NE DEVRAIT PAS", "RECOMMANDE", "PEUT", et "FACULTATIF" en majuscules dans ce document sont à interpréter comme décrit dans le BCP 14, [RFC2119].

Le reste de la terminologie est utilisé comme défini dans la [RFC3775].

2. Déclaration d'applicabilité

Ce mécanisme est utile dans les scénarios où les conditions suivantes sont toutes satisfaites :
- Le nœud mobile et le nœud correspondant sont administrés dans le même domaine.
- Le nœud correspondant a de bonnes raisons de faire confiance aux actions du nœud mobile. En particulier, le nœud correspondant a besoin d'être certain que le nœud mobile ne va pas lancer des attaques d'inondation contre un tiers comme décrit dans la [RFC4226].
- L'effort de configuration relatif à ce mécanisme est acceptable. Les utilisateurs DOIVENT être capables de générer/choisir une valeur suffisamment bonne (voir la [RFC4086]) pour Kcn.
- On désire tirer parti d'une meilleure efficacité ou d'une plus grande assurance de la correction de l'adresse de rattachement offerte via ce mécanisme.
- Ce mécanisme n'est utilisé que pour authentifier les messages de mise à jour de liens (et non, par exemple, des données) de sorte que le volume total de trafic est faible (voir la [RFC4107] et la discussion à la Section 4).

Ce mécanisme peut aussi être utile dans le développement de logiciels, dans les essais, et les diagnostics relatifs à la signalisation de mobilité.

D'une façon générale, le niveau de confiance requis dont le nœud correspondant a besoin pour permettre une Kbm pré calculable avec un nœud mobile est plus souvent trouvé dans des groupes clos relativement petits d'utilisateurs qui sont personnellement familiers les uns les autres, ou qui ont des bases externes pour établir des interactions de confiance. Un exemple typique de scénario où ce mécanisme est applicable est au sein d'une corporation, ou entre des utilisateurs spécifiques. L'application dans l'Internet général n'est normalement pas possible à cause de l'effort exigé pour configurer manuellement les nœuds correspondants. L'application à un opérateur de réseau public n'est normalement pas possible à cause des exigences sur la qualité de confiance des nœuds mobiles.

3. Clé de gestion de lien pré calculée

Un nœud mobile et un nœud correspondant peuvent pré configurer des données utiles pour la création d'une clé de gestion de lien (Kbm, *Binding Management Key*) qui peut alors être utilisée pour autoriser les messages de gestion de liens, en particulier des messages de mise à jour de lien et des accusés de réception de lien. Ces données sont comme suit :
- une clé partagée (Kcn) utilisée pour générer des jetons "keygen", longs d'au moins 20 octets,
- un nom occasionnel à utiliser lors de la génération du jeton d'entretien "keygen",
- un nom occasionnel à utiliser lors de la génération du jeton de rattachement "keygen".

Les jetons "keygen" DOIVENT être générés à partir de la Kcn et les noms occasionnels comme spécifié dans la spécification IPv6 mobile [RFC3775] retournent la capacité d'acheminement. De même, la clé de gestion de lien Kbm doit ensuite être générée à partir des jetons keygen de la même façon que spécifié dans IPv6 mobile [RFC3775]. Les données pré configurées sont associées à l'adresse de rattachement du nœud mobile. Kcn DOIT être généré avec un aléa suffisant (voir la [RFC4086]).

La protection contre la répétition pour les messages de mise à jour de lien en utilisant une Kbm calculée à partir des données pré configurées dépend de la valeur du champ Numéro de séquence dans la mise à jour de lien. Si le nœud correspondant ne conserve pas les informations sur les valeurs utilisées récemment dans ce champ, il peut alors y avoir une opportunité pour qu'un nœud malveillant répète de vieux messages de mise à jour de lien et trompe le nœud correspondant en l'acheminant sur une vieille adresse d'entretien. Pour cette raison, un nœud correspondant qui utilise une Kbm pré calculable DOIT aussi garder trace de la plus récente valeur du champ Numéro de séquence des messages de mise à jour de lien en utilisant la valeur de Kbm pré calculable (par exemple, en s'engageant à une mémorisation stable).

Quand une mise à jour de lien doit être authentifiée en utilisant une telle clé de lien pré calculable (Kbm), la sous option Données d'autorisation de lien DOIT être présente. L'option Indices de nom occasionnel NE DEVRAIT PAS être présente. Si elle est présente, les indices de nom occasionnel fournis DEVRAIENT être ignorés et ne sont pas inclus au titre du calcul des données d'authentification, qui doit être effectué exactement comme spécifié dans la [RFC3775].

4. Considérations sur la sécurité

Un nœud correspondant et un nœud mobile peuvent utiliser une clé de gestion de lien pré calculable (Kbm) pour gérer les exigences d'authentification pour les messages de gestion d'antémémoire de liens. De telles clés doivent être traitées avec

soin pour éviter l'exposition par inadvertance à des menaces discutées dans la [RFC4226]. Les exigences mentionnées dans le présent document sont destinées à assurer la sûreté de la configuration manuelle. En particulier, Kcn DOIT être généré avec un aléa suffisant (voir la [RFC4086]) comme noté à la Section 3.

Les clés configurées manuellement DOIVENT être utilisées conformément à la [RFC4107]. Utilisées en accord avec la déclaration d'applicabilité, et avec les autres mesures de sécurité rendues obligatoires dans la présente spécification, les clés satisferont aux propriétés de ce document. Afin d'assurer la protection contre les attaques de dictionnaire, les informations de sécurité configurées sont destinées à être utilisées SEULEMENT pour l'authentification des messages de mise à jour de lien.

Un nœud mobile DOIT utiliser une valeur différente de Kcn pour chaque nœud dans sa liste de mise à jour de liens, et un nœud correspondant DOIT s'assurer que chaque nœud mobile utilise une valeur différente de Kcn. Cela assure que l'envoyeur d'une mise à jour de lien peut toujours être déterminé de façon univoque. Ceci est nécessaire, car cette méthode d'autorisation ne donne aucune garantie que l'adresse d'entretien donnée soit légitime. Pour la même raison, cette méthode DEVRAIT n'être appliquée qu'entre des nœuds qui sont sous la même administration. La procédure d'acheminement de retour est RECOMMANDÉE pour toute utilisation générale et DOIT être celle par défaut, sauf si l'utilisateur l'outrepasse explicitement en entrant les données pré configurées sus-mentionnées pour un homologue particulier.

La protection contre la répétition pour le mécanisme d'authentification de l'option Données d'autorisation de lien est assurée par le champ Numéro de séquence de la mise à jour de lien. Cette méthode de fourniture de la protection contre la répétition échoue quand les numéros de séquence de mise à jour de lien débordent le compteur de 16 bits (c'est-à-dire, plus de 65 536 utilisations distinctes de Kbm) ou si les numéros de séquence ne sont pas protégés contre les réamorçages. Si le nœud mobile devait envoyer une mise à jour de lien fraîche à son nœud correspondant toutes les heures, 24 heures par jour, chaque jour de l'année, cela exigerait de changer de clés tous les 7 ans. Même si le nœud mobile devait le faire à chaque minute, cela fournirait une protection pour plus d'un mois. Étant donnés les schémas normaux de mobilité, il y a peu de danger de problèmes de répétition ; les nœuds pour lesquels des problèmes pourraient se poser sont supposés utiliser d'autres méthodes que la configuration manuelle de Kcn et des noms occasionnels associés. Quand le champ Numéro de séquence revient à zéro, les parties DEVRAIENT configurer une nouvelle valeur pour Kcn, afin que les nouvelles valeurs de Kbm soient calculées.

Si un nœud correspondant NE garde PAS trace du numéro de séquence pour les messages de mise à jour de lien pour un certain nœud mobile, le nœud correspondant pourrait être trompé et accepter une vieille valeur pour l'adresse d'entretien du nœud mobile. Dans le cas peu probable où cette adresse serait réallouée à un autre nœud IPv6 dans l'intervalle, ce nœud IPv6 serait alors vulnérable à du trafic parasite émanant du nœud correspondant.

Noter que si un nœud était configuré à utiliser le mécanisme spécifié dans le présent document avec un certain homologue , il NE DEVRAIT PAS tenter d'utiliser un autre mécanisme, même si l'homologue le demande ou prétend ne pas prendre en charge le mécanisme du présent document. Ceci est nécessaire pour empêcher les attaques en dégradation d'enchères.

Il n'y a pas de limite supérieure à la durée de vie définie pour le Kbm pré calculable. Comme on l'a noté, la clé va très probablement être assez sûre pendant la durée de vie de l'association de sécurité et utile aux applications entre un nœud mobile et un nœud correspondant qui correspondent aux termes spécifiés dans la Section 2.

5. Remerciements

Merci à tous ceux qui ont revu la discussion de la question n° 146. Merci à Jari Arkko qui a fourni du teste pour l'introduction.

6. Références

6.1 Références normatives

[RFC2119] S. Bradner, "Mots clés à utiliser dans les RFC pour indiquer les niveaux d'exigence", BCP 14, mars 1997. *(MàJ par* RFC8174)

[RFC3775] D. Johnson, C. Perkins, J. Arkko, "Prise en charge de la mobilité dans IPv6", juin 2004. *(P.S.) (Obs., voir* RFC6275)

[RFC4086] D. Eastlake 3rd, J. Schiller, S. Crocker, "Exigences d'aléa pour la sécurité", juin 2005. (*Remplace* RFC1750) (BCP0106)

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

6.2 Références pour information

[RFC4226] D. M'Raihi et autres, "HOTP : Algorithme de mot de passe à utilisation unique fondé sur HMAC", décembre 2005. *(Info.)*

Adresse de l'auteur

Charles E. Perkins
Nokia Research Center
313 Fairchild Drive
Mountain View, CA 94043
USA
téléphone : +1 650 625-2986
fax : +1 650 625-2502
mél : charles.perkins@nokia.com

Déclaration de droits de reproduction

Remerciement
Le financement de la fonction d'édition des RFC est fourni par l'activité de soutien administratif de l'IETF (IASA).