Groupe de travail Réseau
Request for Comments : 4283
Catégorie : Sur la voie de la normalisation
Traduction Claude Brière de L'Isle

A. Patel & K. Leung, Cisco Systems
M. Khalil & H. Akhtar, Nortel Networks
K. Chowdhury, Starent Networks
novembre 2005

Option Identifiant de nœud mobile pour IPv6 mobile (MIPv6)

Résumé
IPv6 mobile (MIPv6, *Mobile IPv6*) définit un nouvel en-tête Mobilité qui est utilisé par les nœuds mobiles, les nœuds correspondants, et les agents de rattachement dans tous les messages relatifs à la création et la gestion des liens. Les nœuds IPv6 mobiles ont besoin d'avoir la capacité de s'identifier en utilisant une identité autre que l'adresse IP de rattachement par défaut. Certains exemples d'identifiants incluent l'identifiant d'accès réseau (NAI, *Network Access Identifier*), le nom de domaine pleinement qualifié (FQDN, *Fully Qualified Domain Name*) l'identifiant international de station mobile (IMSI, *International Mobile Station Identifier*) et le numéro d'abonné mobile (MSISDN, *Mobile Subscriber Number*). Le présent document définit une nouvelle option de mobilité qui peut être utilisée par les entités IPv6 mobiles pour s'identifier dans les messages contenant un en-tête de mobilité.

Table des matières

1. Introduction

La spécification de base de IPv6 mobile [RFC3775] identifie les entités de mobilité en utilisant une adresse IPv6. Il est essentiel d'avoir un mécanisme par lequel les entités de mobilité puissent être identifiées en utilisant d'autres identifiants (par exemple, un identifiant d'accès réseau (NAI, *Network Access Identifier*) [RFC4282], un identifiant international de station mobile (IMSI, *International Mobile Station Identifier*), ou identifiant opaque spécifique de l'application/déploiement).

La capacité d'identifier une entité mobile via des identifiants autres que l'adresse IPv6 peut être développée pour effectuer diverses fonctions, par exemple,

- l'authentification et l'autorisation utilisant une infrastructure existante d'authentification, autorisation et comptabilité (AAA, *Authentication, Authorization, and Accounting*) ou via un centre de registre/authentification de localisation de rattachement (HLR/AuC, *Home Location Register/Authentication Center*)

- l'allocation dynamique d'un point d'ancrage de mobilité,

- l'allocation dynamique d'une adresse de rattachement.

Le présent document définit une option avec un numéro de sous type qui note un type d'identifiant spécifique. Une instance de sous type, le NAI, est définie au paragraphe 3.1. Il est prévu que d'autres identifiants soient définis pour être utilisés à l'avenir dans l'en-tête de mobilité.

Cette option DEVRAIT être utilisée quand l'échange de clés Internet (IKE, *Internet Key Exchange*)/IPsec n'est pas utilisé pour protéger les mises à jour de liens ou les accusés de réception de liens, comme spécifié dans la [RFC3775]. Elle est normalement utilisée avec l'option d'authentification [RFC4285]. Mais cette option peut être utilisée de façon indépendante. Par exemple, l'identifiant peut fournir des services de comptabilité et de facturation.

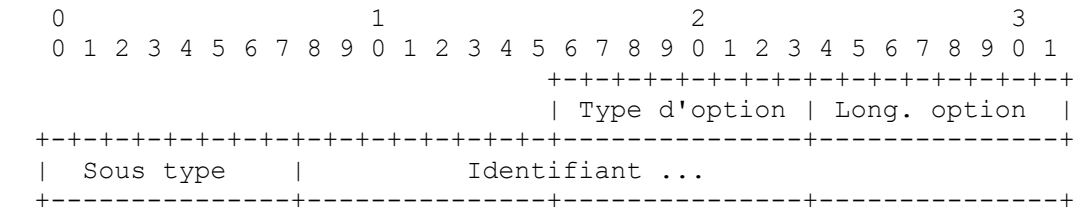
2. Terminologie

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].

3. Option Identifiant de nœud mobile

L'option Identifiant de nœud mobile est un nouveau champ de données facultatif porté dans les messages définis par IPv6 mobile qui comportent l'en-tête Mobilité. Diverses formes d'identifiants peuvent être utilisées pour identifier un nœud mobile (MN, *Mobile Node*). Deux exemples sont un identifiant d'accès réseau (NAI, *Network Access Identifier*) [RFC4282] et un identifiant opaque applicable à une application particulière. Le champ Sous type dans l'option définit le type spécifique d'identifiant.

Cette option peut être utilisée dans les messages de mobilité qui contiennent un en-tête de mobilité. Le champ Sous type dans l'option est utilisé pour interpréter le type spécifique d'identifiant.



Type d'option : MN-ID-OPTION-TYPE a reçu de l'IANA la valeur 8. C'est un identifiant de 8 bits du type d'option Mobilité.

Longueur d'option : entier non signé de 8 bits, représentant la longueur en octets des champs Sous type et Identifiant.

Sous type : le champ Sous type définit le type spécifique d'identifiant inclus dans le champ Identifiant.

Identifiant : identifiant de type de longueur variable, comme spécifié par le champ Sous type de cette option.

Cette option n'a pas d'exigence d'alignement.

3.1 Option Mobilité MN-NAI

L'option Mobilité MN-NAI utilise le format général de l'option Identifiant de nœud mobile comme défini à la Section 3. Cette option utilise la valeur de sous type de 1. L'option Mobilité MN-NAI est utilisée pour identifier le nœud mobile.

L'option Mobilité MN-NAI utilise un identifiant de la forme usager@domaine [RFC4282]. Cette option DOIT être mise en œuvre par les entités qui utilisent la présente spécification.

3.2 Considérations de traitement

La localisation de l'option Identifiant de MN est la suivante : lorsque présente, cette option DOIT apparaître avant toute option en rapport avec l'authentification dans un message contenant un en-tête Mobilité.

4. Considérations sur la sécurité

4.1 Considérations générales

IPv6 Mobile contient déjà un mécanisme pour identifier les nœuds mobiles, l'option Adresse de rattachement [RFC3775]. Par suite, les vulnérabilités de la nouvelle option définie dans le présent document sont similaires à celles qui existent déjà pour IPv6 mobile. En particulier, l'utilisation d'un identifiant permanent stable peut compromettre la confidentialité de l'utilisateur, rendant possible le traçage d'un appareil ou usager particulier quand il se déplace d'une localisation à une autre.

4.2 Considérations de MN-NAI

Comme l'option Identifiant de nœud mobile décrit à la Section 3 révèle l'affiliation de rattachement d'un usager, elle peut aider un attaquant à déterminer l'identité de l'usager, aider l'attaquant à cibler des victimes spécifiques, ou aider à sonder plus avant l'espace de noms d'utilisateur.

Ces vulnérabilités peuvent être traitées par divers mécanismes, tels que ceux mentionnés ci-dessous :

- Chiffrer le trafic à la couche liaison, de façon que les autres utilisateurs sur la même liaison ne voient pas les identifiants. Ce mécanisme n'est d'aucune aide contre des attaques sur le reste du chemin entre le nœud mobile et son agent de rattachement.

- Chiffrer le paquet entier, comme quand on utilise IPsec pour protéger les communications avec l'agent de rattachement [RFC3776].

- Utiliser un mécanisme d'authentification qui permet l'utilisation de NAI de confidentialité [RFC4282] ou temporaires, changeant de "pseudonymes" comme identifiants.

Dans tous les cas, on notera que comme l'option d'identifiant n'est nécessaire que sur le premier enregistrement chez l'agent de rattachement et que les enregistrements suivants peuvent utiliser l'adresse de rattachement, la fenêtre de vulnérabilité de la confidentialité dans ce document est réduite par rapport à la [RFC3775]. De plus, le présent document fait partie d'une solution qui permet d'utiliser l'allocation dynamique des adresses de rattachement. C'est aussi une amélioration de la confidentialité, et cela affecte à la fois les communications avec l'agent de rattachement et avec les nœuds correspondants, qui tous deux doivent avoir l'adresse de rattachement.

5. Considérations relatives l'IANA

Les valeurs pour les nouvelles options de mobilité doivent être allouées à partir de l'espace de numérotation de IPv6 mobile [RFC3775].

L'IANA a alloué la valeur 8 pour le type MN-ID-OPTION-TYPE.

De plus, l'IANA a créé un nouvel espace de noms pour le champ Sous type de l'option Identifiant de nœud mobile. La valeur actuellement allouée est :

1 -- NAI (défini dans la [RFC4282]).

De nouvelles valeurs pour cet espace de noms peuvent être allouées par action de normalisation [RFC2434].

6. Remerciements

Les auteurs tiennent à remercier Basavaraj Patil de sa relecture et ses suggestions sur ce document. Merci à Jari Arkko pour sa relecture et ses suggestions concertant les considérations de sécurité et divers autres aspects du document.

7. 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)

[RFC2434] T. Narten et H. Alvestrand, "Lignes directrices pour la rédaction d'une section Considérations relatives à l'IANA dans les RFC", BCP 26, octobre 1998. *(Rendue obsolète par la* RFC5226)

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

[RFC3776] J. Arkko, V. Devarapalli, F. Dupont, "Utilisation de IPsec pour la protection de la signalisation IPv6 mobile entre nœuds mobiles et agents nominaux", juin 2004. (*MàJ par* RFC4877) *(P.S.)*

[RFC4282] B. Aboba et autres, "L'identifiant d'accès réseau", décembre 2005. *(P.S., Remplacée par* RFC7542)

8. Références pour information

[RFC4285] A. Patel et autres, "Protocole d'authentification pour IPv6 mobile", janvier 2006. *(Information)*

Adresse des auteurs

Kuntal Chowdhury
Starent Networks
30 International Place
Tewksbury, MA 01876
US
téléphone : +1 214-550-1416
mél : kchowdhury@starentnetworks.com

Alpesh Patel
Cisco Systems
170 W. Tasman Drive
San Jose, CA 95134
US
téléphone : +1 408-853-9580
mél : alpesh@cisco.com

Kent Leung
Cisco Systems
170 W. Tasman Drive
San Jose, CA 95134
US
téléphone : +1 408-526-5030
mél : kleung@cisco.com

Mohamed Khalil
Nortel Networks
2221 Lakeside Blvd.
Richardson, TX 75082
US
téléphone : +1 972-685-0574
mél : mkhalil@nortel.com

Haseeb Akhtar
Nortel Networks
2221 Lakeside Blvd.
Richardson, TX 75082
US
téléphone : +1 972-684-4732
mél : haseebak@nortel.com

Déclaration complète de droits de reproduction

Propriété intellectuelle

L'IETF ne prend pas position sur la validité et la portée de tout droit de propriété intellectuelle ou autres droits qui pourraient être revendiqués au titre de la mise en œuvre ou l'utilisation de la technologie décrite dans le présent document ou sur la mesure dans laquelle toute licence sur de tels droits pourrait être ou n'être pas disponible ; pas plus qu'elle ne prétend avoir accompli aucun effort pour identifier de tels droits. Les informations sur les procédures de l'ISOC au sujet des droits dans les documents de l'ISOC figurent dans les BCP 78 et BCP 79.

Des copies des dépôts d'IPR faites au secrétariat de l'IETF et toutes assurances de disponibilité de licences, ou le résultat de tentatives faites pour obtenir une licence ou permission générale d'utilisation de tels droits de propriété par ceux qui mettent en œuvre ou utilisent la présente spécification peuvent être obtenues sur répertoire en ligne des IPR de l'IETF à http://www.ietf.org/ipr .

L'IETF invite toute partie intéressée à porter son attention sur tous copyrights, licences ou applications de licence, ou autres droits de propriété qui pourraient couvrir les technologies qui peuvent être nécessaires pour mettre en œuvre la présente norme. Prière d'adresser les informations à l'IETF à ietf-ipr@ietf.org .

Remerciement

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