Groupe de travail Réseau
Request for Comments : 5269
Catégorie : Sur la voie de la normalisation
Traduction Claude Brière de L'Isle

J. Kempf, DoCoMo Labs USA
R. Koodli, Starent Networks
juin 2008

Distribution d'une clé symétrique de transfert intercellulaire rapide IPv6 mobile (FMIPv6) avec la découverte de voisin sécurisée (SEND)

Statut du présent mémoire

Le présent document spécifie un protocole Internet sur la voie de la normalisation pour la communauté de l'Internet. Il appelle à la discussion et à des suggestions pour son amélioration. Prière de se référer à l'édition actuelle des "Normes officielles des protocoles de l'Internet" (STD 1) pour connaître l'état de normalisation et le statut de ce protocole. La distribution du présent mémoire n'est soumise à aucune restriction.

Résumé

IPv6 mobile rapide exige qu'une mise à jour de lien rapide soit sécurisée en utilisant une association de sécurité partagée entre un routeur d'accès et un nœud mobile afin d'éviter certaines attaques. Dans le présent document, une méthode pour provisionner une clé partagée du routeur d'accès au nœud mobile est définie pour protéger cette signalisation. Le nœud mobile génère une paire de clés publique/privée en utilisant le même algorithme de clé publique que pour SEND (RFC3971). Le nœud mobile envoie la clé publique au routeur d'accès. Le routeur d'accès chiffre une clé de transfert partagée en utilisant la clé publique et la renvoie au nœud mobile. Le nœud mobile déchiffre la clé de transfert partagée en utilisant la clé privée correspondante, et la clé de transfert est alors disponible pour générer un authentificateur sur une mise à jour de lien rapide. Le nœud mobile et le routeur d'accès utilisent la sollicitation de routeur pour les annonces de mandataire et l'annonce de routeur mandataire provenant de IPv6 mobile rapide pour l'échange de clé. Les messages d'échange de clé sont obligés d'avoir la sécurité SEND ; c'est-à-dire, l'adresse de source est une adresse générée cryptographiquement (CGA, *Cryptographically Generated Address*) et les messages sont signés en utilisant la clé privée de CGA du nœud envoyeur. Cela permet au routeur d'accès, avant de fournir la clé de transfert partagée, de vérifier l'autorisation du nœud mobile de réclamer l'adresse, de sorte que la précédente CGA d'entretien dans la mise à jour de lien rapide peut agir comme nom de la clé.

Table des matières

1. Introduction

Dans IPv6 mobile rapide (FMIPv6, *Fast Mobile IPv6*) [RFC5268], une mise à jour de lien rapide (FBU, *Fast Binding Update*) est envoyée d'un nœud mobile (MN, *Mobile Node*) qui est en train de faire un transfert IP, au précédent routeur d'accès (AR, *Access Router*). La FBU cause un changement d'acheminement de sorte que le trafic envoyé à la précédente adresse d'entretien du MN sur la précédente liaison de l'AR est tunnelé à la nouvelle adresse d'entretien sur la nouvelle liaison de l'AR. Seul un MN autorisé à réclamer l'adresse devrait être capable de changer l'acheminement pour la précédente adresse d'entretien. Si cette autorisation n'est pas établie, un attaquant peut rediriger à son gré le trafic d'un MN victime.

Dans le présent document, est défini un mécanisme léger par lequel une clé de transfert partagée pour sécuriser FMIP peut être provisionnée sur le MN par l'AR. Le mécanisme utilise SEND [RFC3971] et une paire de clés publique/privée supplémentaire, générée sur le MN en utilisant le même algorithme de clé publique que SEND, pour chiffrer/déchiffrer une clé de transfert partagée envoyée de l'AR au MN. Le provisionnement de clé survient à un moment arbitraire avant le transfert, supprimant ainsi tout impact sur les performances du processus de transfert. L'échange de messages entre le MN et l'AR pour provisionner la clé de transfert est obligatoirement protégé par SEND ; c'est-à-dire que l'adresse de source pour les messages de provisionnement de clé doit être une CGA et les messages doivent être signés avec la clé privée de la CGA. Cela permet à l'AR d'établir l'autorisation au MN de fonctionner sur la CGA. L'AR utilise la CGA pour désigner la clé de transfert. La paire de clés SEND est cependant indépendante de la paire de clés de chiffrement/déchiffrement de transfert et de la clé de transfert réelle. Une fois que la clé de transfert partagée a été établie, quand le MN entreprend un transfert IP, le MN génère un code d'authentification de message (MAC, *Message Authentication Code*) d'autorisation sur la FBU. La précédente CGA d'entretien incluse dans la FBU est utilisée par l'AR pour trouver la bonne clé de transfert pour vérifier l'autorisation.

Les clés de transfert sont une instance du principe architectural de clé construite à dessein [PBK].

1.1 Terminologie

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

De plus, la terminologie suivante est utilisée :

Clé publique de CGA : clé publique utilisée pour générer la CGA conformément à la [RFC3972].

Clé privée de CGA : clé privée correspondant à la clé publique de CGA.

Clé publique de chiffrement de clé de transfert : clé publique générée par le MN et envoyé à l'AR en cours pour chiffrer la clé de transfert partagée.

Clé privée de chiffrement de clé de transfert : clé privée correspondant à la clé publique de chiffrement de clé de transfert, détenue par le MN.

2. Vue d'ensemble du protocole

2.1 Brève revue de SEND

SEND protège contre diverses menaces sur la résolution d'adresse de liaison locale (aussi appelés la découverte de voisin) et la découverte du routeur de dernier bond (AR) dans IPv6 [RFC3756]. Ces menaces ne sont pas exclusives aux réseaux sans fil, mais elles sont généralement plus faciles à monter sur certains réseaux sans fil parce que la liaison entre les points d'accès et le MN ne peut pas être physiquement sécurisée.

SEND utilise des CGA afin de sécuriser la signalisation de la découverte de voisin [RFC3972]. En bref, une CGA est formée en hachant ensemble le préfixe de sous réseau IPv6 pour le sous réseau d'un nœud, un nom occasionnel aléatoire, et une clé publique RSA, appelée la clé publique de CGA. La clé privée de CGA est utilisée pour signer un message d'annonce de voisin (NA, *Neighbor Advertisement*) envoyé pour résoudre l'adresse de couche de liaison en adresse IPv6. La combinaison de la CGA et de la signature sur la NA prouve au nœud receveur l'autorisation de l'envoyeur de réclamer

l'adresse. Le nœud peut opportunément générer une ou plusieurs clés spécifiquement pour SEND, ou il peut utiliser une clé certifiée qu'il distribue plus largement.

2.2 Vue d'ensemble du protocole

Le protocole utilise l'échange de sollicitation de routeur sécurisée par SEND pour les annonces de mandataire (RtSolPr, *Router Solicitation for Proxy Advertisement*)/annonce de routeur mandataire (PrRtAdv, *Proxy Router Advertisement*) [RFC5268] entre le MN et l'AR pour transporter une clé de transfert partagée chiffrée de l'AR au MN. D'abord, le MN génère la paire de clés et les adresses de CGA associées nécessaires pour que le MN puisse employer SEND. Ensuite, le MN génère une paire de clés publique/privée pour chiffrer/déchiffrer la clé de transfert partagée, en utilisant le même algorithme de clé publique qu'utilisé pour SEND. Le MN envoie alors un message RtSolPr avec une option Demande de clé de transfert contenant la clé publique de chiffrement de clé de transfert. L'adresse de source du message RtSolPr est la CGA d'entretien du MN sur la liaison de l'AR, le message RtSolPr est signé avec la clé de CGA du MN, et contient l'option Paramètres de CGA, conformément à la [RFC3971]. L'AR vérifie le message en utilisant SEND, puis utilise la clé publique de chiffrement de clé de transfert pour chiffer une clé de transfert partagée, qui est incluse avec le PrRtAdv dans l'option de réponse de clé de transfert. Le MN déchiffre la clé de transfert partagée et l'utilise pour établir un MAC d'autorisation quand il envoie une FBU à l'AR précédent.

3. Provisionnement et utilisation de la clé de tréansfert

3.1 Envoi des sollicitations de routeur pour les annonces de mandataire

Un moment avant le transfert, le MN DOIT générer une paire de clés publique/privée de clé de transfert, en utilisant exactement le même algorithme de clé publique avec exactement les mêmes paramètres (taille de clé, etc.) que pour SEND [RFC3971]. Le MN peut réutiliser la paire de clés sur différents routeurs d'accès mais NE DOIT PAS utiliser la paire de clés pour un autre chiffrement ou opération de signature. Afin d'empêcher la cryptanalyse, la paire de clés DEVRAIT être éliminée après soit une durée de HKEPK-LIFETIME, soit un nombre HKEPK-HANDOVERS de transferts, selon ce qui arrive en premier. Voir au paragraphe 3.7 les définitions des constantes du protocole.

Le MN DOIT envoyer une sollicitation de routeur pour annonce de mandataire (RtSolPr) contenant une option Demande de clé de transfert avec la clé publique de chiffrement de transfert. Une CGA pour le MN DOIT être l'adresse de source sur le paquet, et le MN DOIT inclure l'option SEND CGA et l'option SEND Signature avec le paquet, comme spécifié dans la [RFC3971]. La signature SEND couvre tous les champs dans la RtSolPr, incluant les adresses de 128 bits de source et destination et la somme de contrôle ICMP comme décrit dans la RFC 3971, sauf pour l'option Signature elle-même. Le MN règle aussi le champ d'extension Type d'algorithme (AT, *Algorithm Type*) d'authentification de transfert dans l'option Demande de clé de transfert à l'algorithme d'authentification de FBU préféré du MN. Le nom occasionnel SEND DOIT aussi être inclus pour la protection contre la répétition.

3.2 Réception de sollicitation de routeur pour annonce de mandataire et envoi d'annonce de routeur mandaire

Quand un AR capable de FMIPv6 avec SEND reçoit une RtSolPr d'un MN protégé avec SEND et incluant une option Demande de clé de transfert, l'AR DOIT d'abord valider la RtSolPr en utilisant SEND comme décrit dans la RFC 3971. Si la RtSolPr ne peut pas être validée, l'AR NE DOIT PAS inclure d'option Réponse de clé de transfert dans la réponse. Aussi, l'AR NE DOIT PAS changer un enregistrement de clé existant pour l'adresse, car le message peut être une tentative d'un attaquant pour perturber les communications pour un MN légitime. L'AR DEVRAIT répondre à la RtSolPr mais NE DOIT PAS effectuer de provisionnement de clé de transfert.

Si la RtSolPr peut être validée, l'AR DOIT alors déterminer si la CGA est déjà associée à une clé de transfert partagée. Si la CGA est associée à une clé de transfert existante, l'AR DOIT retourner la clé de transfert existante au MN. Si la CGA n'a pas une clé de transfert partagée, l'AR DOIT construire une clé de transfert partagée comme décrit au paragraphe 3.6. L'AR DOIT chiffrer la clé de transfert avec la clé publique de chiffrement de clé de transfert incluse dans l'option Demande de clé de transfert. L'AR DOIT insérer la clé de transfert chiffrée dans une option Réponse de clé de transfert et DOIT attacher l'option Réponse de clé de transfert au message PrRtAdv. La durée de vie de la clé, HK-LIFETIME, DOIT aussi être incluse dans l'option Réponse de clé de transfert. L'AR DEVRAIT régler le champ AT de l'option Clé de transfert au type d'algorithme préféré du MN indiqué dans le champ AT de l'option Demande de clé de transfert, si elle est prise en charge ; autrement, l'AR DOIT choisir un algorithme d'authentification qui soit de force équivalente ou supérieure, et régler le champ à cela. L'AR DOIT aussi inclure le nom occasionnel SEND provenant du message RtSolPr pour la protection contre la répétition. L'AR DOIT avoir un certificat convenable pour un routeur à capacité SEND, prendre en charge la découverte de certificat SEND, et inclure une option CGA SEND et une option Signature SEND dans les messages PrRtAdv qu'il envoie. De même, les nœuds mobiles DOIVENT être configurés avec une ou plusieurs ancres de confiance SEND afin

qu'ils puissent vérifier ces messages. La signature SEND couvre tous les champs dans le message PrRtAdv, incluant les 128 bits des adresses de source et destination et la somme de contrôle ICMP comme décrit dans la RFC 3971, sauf pour l'option Signature elle-même. La PrRtAdv est alors renvoyée en envoi individuel au MN à la CGA d'entretien du MN qui était l'adresse de source sur la RtSolPr. La clé de transfert DOIT être mémorisée par l'AR pour une utilisation future, indexée par la CGA, et le type d'algorithme d'authentification (c'est-à-dire, la résolution du traitement du champ AT) et HK-LIFETIME DOIVENT être enregistrés avec la clé.

3.3 Réception d'annonce de routeur mandataire

À réception de une ou plusieurs PrRtAdv sécurisées avec SEND et ayant l'option Réponse de clé de transfert, le MN DOIT d'abord valider les PrRtAdv comme décrit dans la RFC 3971. Normalement, le MN va avoir obtenu le chemin de certification du routeur pour valider un RA avant d'envoyer la PrRtSol et le MN DOIT vérifier que la clé utilisée pour signer la PrRtAdv est la clé publique certifiée du routeur. Si le MN n'a pas le chemin de certification du routeur en antémémoire, il DOIT utiliser les messages SEND CPS/CPA pour obtenir le chemin de certification pour valider la clé. Si une clé certifiée provenant du routeur n'a pas été utilisée pour signer le message, le message DOIT être éliminé.

Parmi les messages validés, le MN DEVRAIT en choisir un avec un fanion AT dans l'option Réponse de clé de transfert indiquant un algorithme d'authentification que le MN prend en charge. À partir de ce message, le MN DOIT déterminer quelle clé publique de chiffrement de clé de transfert utiliser dans le cas où le MN en aurait plus d'une. Le MN trouve la bonne clé publique à utiliser en confrontant le nom occasionnel SEND de la RtSolPr. Si aucune correspondance ne se produit, le MN DOIT éliminer la PrRtAdv. Le MN DOIT utiliser la clé privé correspondante pour déchiffrer la clé de transfert en utilisant sa clé privée de chiffrement de clé de transfert, et mémoriser la clé de transfert pour une utilisation ultérieure, nommée avec la CGA de l'AR, avec le type d'algorithme et HK-LIFETIME. Le MN DOIT utiliser le type d'algorithme retourné indiqué dans la PrRtAdv. Le MN DOIT indexer les clés de transfert avec les adresses IPv6 de l'AR, auxquelles le MN envoie plus tard la FBU, et la CGA de la MN à laquelle la clé de transfert s'applique. Cela permet au MN de choisir la clé appropriée quand il communique avec l'AR précédent. Avant l'expiration de HK-LIFETIME, le MN DOIT demander une nouvelle clé à l'AR si le service FMIPv6 est encore exigé du routeur.

Si plus d'un routeur répond à la RtSolPr, le MN PEUT garder trace de toutes ces clés. Si aucune des PrRtAdv ne contient un indicateur de type d'algorithme correspondant à un algorithme que prend en charge le MN, il PEUT renvoyer la RtSolPr en demandant un algorithme différent, mais pour prévenir les attaques en dégradation provenant de routeurs compromis, le MN NE DEVRAIT PAS demander un algorithme plus faible que dans sa demande d'origine.

3.4 Envoi de FBU

Quand le MN a besoin de signaler l'AR précédent (PAR, *Previous AR*) en utilisant une FBU FMIPv6, le MN DOIT utiliser la clé de transfert et l'algorithme d'authentification correspondant pour générer un authentificateur pour le message. Le MN DOIT choisir la clé appropriée pour le PAR en utilisant la CGA du PAR et la CGA d'entretien précédente du MN sur la liaison du PAR. Comme défini par FMIPv6 [RFC5268], le MN DOIT générer le MAC d'authentification en utilisant la clé de transfert et l'algorithme approprié et DOIT inclure le MAC dans le message de FBU. Comme spécifié par FMIPv6, le MN DOIT inclure l'ancienne CGA d'entretien dans une option Adresse de rattachement. Le document FMIPv6 donne plus de détails sur la construction de l'authentificateur sur la FBU.

3.5 Réception de FBU

Quand le PAR reçoit un message de FBU contenant un authentificateur, le PAR DOIT trouver la clé de transfert correspondante en utilisant comme indice la CGA d'entretien du MN dans l'option Adresse de rattachement. Si une clé de transfert est trouvée, le PAR DOIT utiliser la clé de transfert et l'algorithme approprié pour vérifier l'authentificateur. Si la clé de transfert n'est pas trouvée, le PAR NE DOIT PAS changer la transmission de la CGA d'entretien. Le document FMIPv6 [RFC5268] fournit plus de détails sur la façon dont l'AR traite une FBU contenant un authentificateur.

3.6 Génération et durée de vie de clé

L'AR DOIT générer au hasard une clé ayant une force suffisante pour correspondre à l'algorithme d'authentification. Certains algorithmes d'authentification spécifient une taille de clé exigée. L'AR DOIT générer une clé unique pour chaque clé publique de CGA, et DEVRAIT veiller à ce que la génération de clé soit sans corrélation entre les clés de transfert, et entre les clés de transfert et les clés de CGA. L'algorithme réel utilisé pour générer la clé n'est pas important pour l'interopérabilité car seul l'AR génère la clé ; le MN l'utilise simplement.

Un PAR NE DEVRAIT PAS éliminer la clé de transfert immédiatement après l'avoir utilisée si elle est encore valide. Il est possible que le MN puisse subir un mouvement rapide à un autre AR avant l'achèvement de la mise à jour de lien IPv6 mobile sur le PAR, et le MN PEUT en conséquence initialiser une autre optimisation de transfert suivante pour déplacer le trafic du PAR à un autre nouveau PAR. La durée par défaut pour garder la clé valide correspond à la durée par défaut pendant laquelle la transmission du PAR au nouvel AR est effectuée pour FMIP. Le document FMIPv6 [RFC5268] fournit plus de détails sur la durée de transmission FMIP par défaut.

Si le MN retourne à un PAR avant l'expiration de la clé de transfert, le PAR PEUT envoyer et le MN PEUT recevoir la même clé de transfert que précédemment retournée, si le MN génère la même CGA pour son adresse d'entretien. Cependant, le MN NE DOIT PAS supposer qu'il peut continuer d'utiliser la vieille clé sans recevoir à nouveau la clé de transfert du PAR. Le MN DEVRAIT éliminer la clé de transfert après l'achèvement de la mise à jour de lien MIPv6 sur le nouvel AR. Le PAR DOIT éliminer la clé après l'arrivée à expiration de la transmission FMIPv6 pour la précédente adresse d'entretien ou quand HK-LIFETIME arrive à expiration.

3.7 Constantes du protocole

Voici les constantes du protocole avec leurs valeurs par défaut suggérées :

HKEPK-LIFETIME : durée de vie maximum pour la clé publique de chiffrement de clé de transfert. 12 heures par défaut.

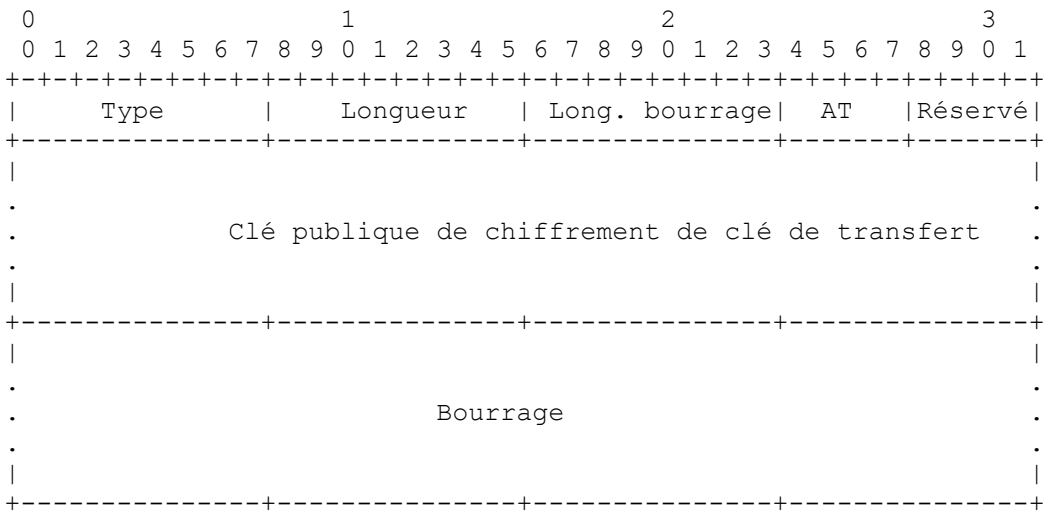
HKEPK-HANDOVERS : nombre maximum de transferts pour lequel la clé publique de chiffrement de clé de transfert devrait être réutilisée. 10 par défaut.

HK-LIFETIME : durée de vie maximum pour la clé de transfert. 12 heures par défaut (43 200 secondes).

4. Formats de message

4.1. Option Demande de clé de transfert

L'option Demande de clé de transfert est une option standard de la découverte de voisin IPv6 [RFC4861] en format de TLV. L'option Demande de clé de transfert est incluse dans le message RtSolPr avec l'option SEND CGA, l'option RSA Signature, et l'option Nom occasionnel.



Champs :

Type : 27

Longueur : longueur de l'option en unités de 8 octets, incluant les champs Type et Longueur. La valeur 0 est invalide. Le receveur DOIT éliminer un message qui contient cette valeur.

Longueur de bourrage : nombre d'octets de bourrage au delà de la fin du champ Clé publique de chiffrement de clé de transfert mais dans la longueur spécifiée par le champ Longueur. Les octets de bourrage DOIVENT être réglés à zéro par l'envoyeur et ignorés par le receveur.

AT : champ de type d'algorithme de 4 bits décrivant l'algorithme utilisé par FMIPv6 pour calculer l'authentificateur. Voir les détails dans la [RFC5268].

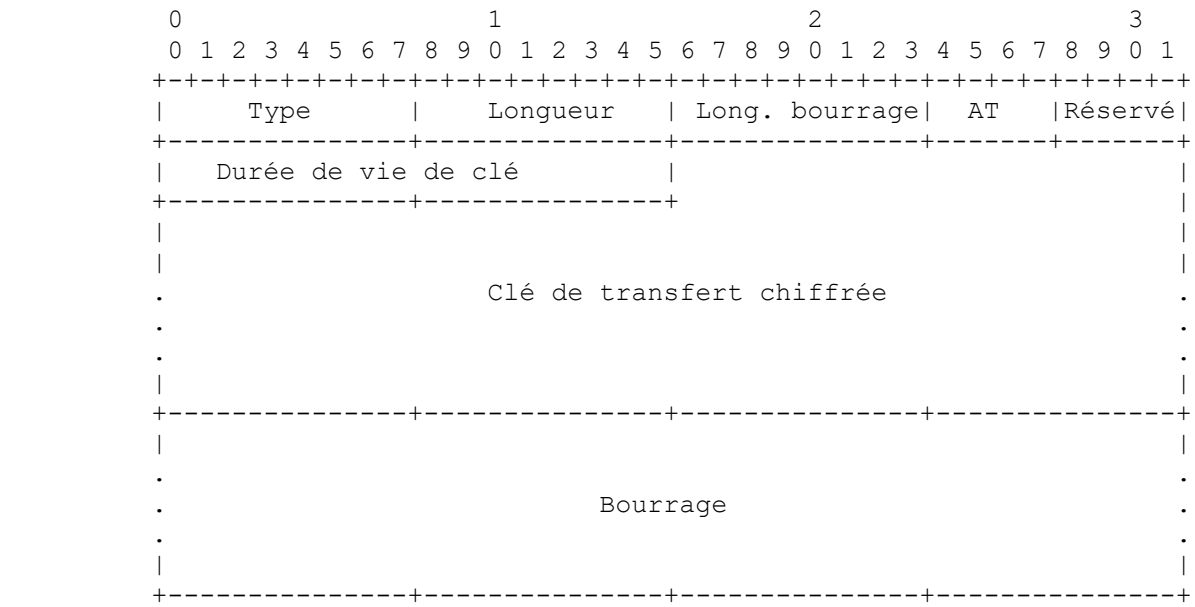
Réservé : champ de 4 bits réservé pour une utilisation future. La valeur DOIT être initialisée à zéro par l'envoyeur et DOIT être ignorée par le receveur.

Clé publique de chiffrement de clé de transfert : la clé elle-même . Elle DOIT être formatée selon la même spécification que la clé de CGA dans l'option Paramètres de CGA [RFC3972] du message, et DOIT avoir les mêmes paramètres que la clé de CGA.

Bourrage : champ de longueur variable rendant la longueur de l'option un multiple de 8, contenant autant d'octets que spécifié dans le champ Longueur de bourrage.

4.2 Option Réponse de clé de transfert

L'option Réponse de clé de transfert est une option standard de la découverte de voisin IPv6 [RFC4861] en format de TLV. L'option Réponse de clé de transfert est incluse dans le message PrRtAdv avec l'option SEND CGA, l'option RSA Signature, et l'option Nom occasionnel.



Champs :

Type : 28

Longueur : longueur de l'option en unités de 8 octets, incluant les champs Type et Longueur. La valeur 0 est invalide. Le receveur DOIT éliminer un message contenant cette valeur.

Longueur de bourrage : nombre d'octets de bourrage au delà de la fin du champ Clé publique de chiffrement de clé de transfert mais dans la longueur spécifiée par le champ Longueur. Les octets de bourrage DOIVENT être réglés à zéro par l'envoyeur et ignorés par le receveurs.

AT : champ de type d'algorithme de 4 bits décrivant l'algorithme utilisé par FMIPv6 pour calculer l'authentificateur. Voir les détails dans la [RFC5268].

Réservé : champ de 4 bits réservé pour une utilisation future. La valeur DOIT être initialisée à zéro par l'envoyeur et DOIT être ignorée par le receveur.

Durée de vie de clé : durée de vie de la clé de transfert, HK-LIFETIME, en secondes.

Clé de transfert chiffrée : clé de transfert partagée, chiffrée avec la clé publique de chiffrement de clé de transfert du MN, en utilisant le format RSAES-PKCS1-v1_5 [RFC3447].

Bourrage : champ de longueur variable rendant la longueur de l'option un multiple de 8, contenant autant d'octets que spécifié dans le champ Longueur de bourrage.

5. Considérations pour la sécurité

Le présent document décrit un protocole de provisionnement de clé partagée pour le protocole d'optimisation de transfert FMIPv6. Le protocole de provisionnement de clé utilise une clé publique générée avec le même algorithme de clé publique que SEND pour amorcer une clé partagée pour les changements d'autorisation dus aux transferts associés à l'ancienne adresse du MN sur le PAR. Les considérations générales de sécurité impliquant les CGA s'appliquent au protocole décrit dans le présent document, voir dans la [RFC3972] une discussion des considérations de sécurité pour les CGA. Ce protocole est sujet aux mêmes risques d'attaques en répétition et de déni de service (DoS) en utilisant RtSolPr que le protocole SEND [RFC3971] pour RS. Les mesures recommandées dans la RFC 3971 pour atténuer les attaques en répétition et les attaques de DoS s'appliquent aussi ici. Une considération supplémentaire est quand générer la clé de transfert sur l'AR. Pour éviter les attaques en dégradation d'état, la clé de transfert NE DEVRAIT PAS être générée avant que le traitement SEND vérifie l'origine de la RtSolPr. Les attaques en dégradation d'état peuvent être contrées par des techniques comme la limitation du taux de RtSolPr, la restriction de la quantité d'état réservé pour les sollicitations non résolues, et une gestion habile de l'antémémoire. Ces techniques sont les mêmes qu'utilisées dans la mise en œuvre de la découverte de voisin.

Pour les autres considérations sur la sécurité de FMIPv6, prière de se reporter au document FMIPv6 [RFC5268].

6. Considérations relatives à l'IANA

L'IANA a alloué les codes de type d'option Découverte de voisin IPv6 pour les deux nouvelles options de découverte de voisin IPv6, l'option Demande de clé de transfert (27) et l'option Réponse de clé de transfert (28), définies dans le présent document.

7. Références

7.1 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)

[RFC3447] J. Jonsson et B. Kaliski, "Normes de cryptographie à clés publiques (PKCS) n° 1 : Spécifications de la cryptographie RSA version 2.1", février 2003. *(Obsolète, remplacée par* RFC8017) *(Information)*

[RFC3971] J. Arkko et autres, "Découverte de voisin sûre (SEND)", mars 2005. (*MàJ par* RFC6494) *(P.S.)*

[RFC3972] T. Aura, "Adresses générées cryptographiquement (CGA)", mars 2005. (*MàJ par* RFC4581, RFC4982) *(P.S.)*

[RFC4861] T. Narten et autres, "Découverte du voisin pour IP version 6 (IPv6)", septembre 2007. (*Remplace* RFC2461) *(D.S. ; MàJ par* RFC8028, RFC8319, RFC8425, RFC9131)

[RFC5268] R. Koodli, éd., "Transferts intercellulaires rapides pour IPv6 mobile", juin 2008. (*Remplace* RFC4068, *remplacée par* RFC5568) *(P.S.)*

7.2 Références pour information

[RFC3756] P. Nikander, éd., "Modèles de confiance et menaces pour la découverte de voisin IPv6 (ND)", mai 2004. *(Information)*

[PBK] S. Bradner, A. Mankin, J. Schiller, "A Framework for Purpose-Built Keys (PBK)", Travail en cours, juin 2003.

Adresse des auteurs

James Kempf
DoCoMo Labs USA
3240 Hillview Avenue
Palo Alto, CA 94303
USA
téléphone : +1 650 496 4711
mél : kempf@docomolabs-usa.com

Rajeev Koodli
Starent Networks
30 International Place
Tewksbury, MA 01876
USA
téléphone : +1 408 735 7679
mél : rkoodli@starentnetworks.com

Déclaration complète de droits de reproduction