Groupe de travail Réseau
Request for Comments : 4423
Catégorie : Information
Traduction Claude Brière de L'Isle

R. Moskowitz, ICSA Labs, Cybertrust, Inc.
P. Nikander, Ericsson Research Nomadic Lab
mai 2006

Architecture du protocole d'identité d'hôte (HIP)

Statut du présent mémoire
Le présent document apporte des informations pour la communauté Internet. Il ne spécifié aucune sorte de norme de l'Internet". La distribution du présent mémoire n'est soumise à aucune restriction.

Résumé
Le présent mémoire décrit un instantané du raisonnement qui sous-tend une proposition de nouvel espace de noms, l'espace de noms Identité d'hôte, et une nouvelle couche de protocole, le protocole d'identité d'hôte (HIP, *identité d'hôte Protocol*), entre les couches d'inter réseautage et de transport. On présente ici les bases des espaces de noms actuels, leurs forces et leurs faiblesses, et comment un nouvel espace de noms va ajouter à leur exhaustivité. Les rôles de ce nouvel espace de noms dans les protocoles sont définis. Le mémoire décrit les pensées des auteurs à la fin 2003. L'architecture peut avoir évolué depuis. Ce document représente un point stable dans l'évolution de sa compréhension.

Table des matières

1. Déclinatoire de responsabilité

L'objet du présent mémoire est de fournir un point de référence stable dans le développement de l'architecture du protocole d'identité d'hôte. Ce mémoire décrit les pensées des auteurs à la fin de 2003 ; leurs idées peuvent avoir évolué depuis. Occasionnellement, ce mémoire peut être confus ou contradictoire. Ceci est (partiellement) intentionnel, et reflète la nature d'instantané du mémoire.

Cette RFC n'est candidate à aucun niveau de norme de l'Internet. L'IETF décline toute prétention que la présente RFC soit convenable à quelque objet que ce soit et note que la décision de la publier ne se fonde pas sur une relecture de l'IETF. Cependant, les idées avancées dans cette RFC ont généré un intérêt significatif, incluant la formation du groupe de travail HIP de l'IETF et du groupe de recherche HIP de l'IRTF. Ces groupes sont supposés générer d'autres documents, partageant leurs découvertes avec la communauté Internet toute entière.

2. Introduction

L'Internet a deux espaces de noms mondiaux importants : les adresses du protocole Internet (IP, *Internet Protocol*) et les noms du service des noms de domaine (DNS, *Domain Name Service*). Ces deux espaces de noms ont un ensemble de caractéristiques et d'abstractions qui ont permis à l'Internet d'être ce qu'il est aujourd'hui. Ils ont aussi un certain nombre de faiblesses. Fondamentalement, comme c'est tout ce que nous avons, nous essayons d'en faire trop avec eux. La surcharge sémantique et les extensions de fonctionnalités ont largement compliqué ces espaces de noms.

L'espace de noms proposée "Identité d'hôte" comble un trou important entre les espaces de noms IP et DNS. L'espace de noms Identité d'hôte consiste en des identifiants d'hôte (HI, *Host Identifier*). Un identifiant d'hôte est par nature cryptographique ; il est la clé publique d'une paire de clés asymétrique. Chaque hôte va avoir au moins une Identité d'hôte, mais il va normalement en avoir plus d'une. Chaque identité d'hôte identifie de façon univoque un seul hôte ; c'est-à-dire, deux hôtes n'ont pas la même identité d'hôte. L'identité d'hôte, et l'identifiant d'hôte correspondant, peuvent être soit publics (par exemple, publié dans le DNS) soit non publiés. Les systèmes clients vont tendre à avoir des identités à la fois publiques et non publiées.

Il y a une différence subtile mais importante entre les identités d'hôte et les identifiants d'hôtes. Une identité se réfère à l'entité abstraite identifiée. Un identifiant, quant à lui, se réfère au schéma de bits concret qui est utilisé dans le processus d'identification.

Bien que les identifiants d'hôte puissent être utilisés dans de nombreux systèmes d'authentification, comme le protocole d'échange de clés Internet version 2 (IKEv2, *Internet Key Exchange version 2*) [RFC4306], l'architecture présentée introduit un nouveau protocole, appelé le protocole d'identité d'hôte (HIP), et un échange cryptographique, appelé l'échange de base HIP ; voir aussi la Section 8. Les protocoles HIP fournissent des formes limitées de confiance entre systèmes, une mobilité améliorée, le multi rattachement, le changement dynamique d'adresse IP ; ils aident à la traduction/transition de protocole, et réduisent certains types d'attaques de déni de service (DoS).

Quand HIP est utilisé, le trafic de charge utile réel entre deux hôtes HIP est normalement, mais pas nécessairement, protégé avec IPsec. Les identités d'hôte sont utilisées pour créer les associations de sécurité IPsec (SA, *Security Association*) nécessaires et pour authentifier les hôtes. Quand IPsec est utilisé, les paquets IP de charge utile réels ne diffèrent en aucune façon des paquets IP standard protégés par IPsec.

3. Terminologie

3.1 Termes communs à d'autres documents

clé publique : clé publique d'une paire de clés de chiffrement asymétrique. Utilisée comme identifiant connu publiquement pour l'authentification d'identité cryptographique .

clé privée : clé privée ou secrète d'une paire de clés de chiffrement asymétrique. Supposée n'être connue que de la partie identifiée par la clé publique correspondante. Utilisée par la partie identifiée pour authentifier son identité auprès des autres parties.

paire de clés publiques : paire de clés de chiffrement asymétrique consistant en clés |publiques et privées. Par exemple, les paires de clés Rivest-Shamir-Adelman (RSA) et de l'algorithme de signature numérique (DSA, *Digital Signature Algorithm*) sont de telles paires de clés.

point d'extrémité : entité communicante. Pour des raisons historiques, le terme "plate-forme de calcul" est utilisé dans le présent document comme synonyme (en gros) de point d'extrémité.

3.2 Termes spécifiques des documents HIP

On notera que beaucoup des termes définis ici sont tautologiques, auto référents, ou définis par des références circulaires aux autres termes. Ceci est dû à la nature succincte des définitions. Voir plus loin dans le document des explications plus élaborées.

plate-forme de calcul : entité capable de communiquer et calculer, par exemple, un ordinateur. Voir la définition de "point d'extrémité" ci-dessus.

échange de base HIP : protocole de chiffrement ; voir aussi la Section 8.

paquet HIP : paquet IP qui porte un message de "protocole d'identité d'hôte".

identité d'hôte : concept abstrait alloué à une "plate-forme de calcul". Voir "identifiant d'hôte", ci-dessous.

espace de noms d'identité d'hôte : espace de noms formé par tous les identifiants d'hôte possibles.

protocole d'identité d'hôte : protocole utilisé pour porter et authentifier les identifiants d'hôte et autres informations.

étiquette d'identité d'hôte : bloc de données de 128 bits créé en prenant un hachage cryptographique d'un identifiant d'hôte.

identifiant d'hôte : clé publique utilisée comme nom pour une identité d'hôte.

identifiant à portée locale : bloc de données de 32 bits notant une identité d'hôte.

identifiant d'hôte public et identité publique : identifiant d'hôte publié ou publiquement connu utilisé comme nom public pour une identité d'hôte, et l'identité correspondante.

identifiant d'hôte non publié : identifiant d'hôte qui n'est pas placé dans un répertoire public, et l'identité d'hôte correspondante. Les identités d'hôte non publiées sont par nature de courte durée de vie, étant souvent remplacées et éventuellement utilisées une seule fois.

mécanisme de rendez-vous : mécanisme utilisé pour localiser les hôtes mobiles sur la base de leur étiquette d'identité d'hôte (HIT, *Host Identity Tag*).

4. Fondements

L'Internet est construit à partir de trois principaux composants : les plates-formes de calcul (points d'extrémité), l'infrastructure de transport de paquets (c'est-à-dire, l'inter réseautage) et les services (applications). L'Internet existe pour servir deux principaux composants : des personnes et des services robotisés (des personnes fondées sur le silicium, si vous préférez). Tous ces composants ont besoin d'être nommés afin d'interagir d'une manière adaptable. On se concentre ici sur la désignation des plates-formes de calcul et des éléments de transport de paquets.

Il y a deux principaux espaces de noms en usage dans l'Internet pour ces composants : les numéros IP et les noms de domaines. Les noms de domaines fournissent des noms alloués de façon hiérarchique pour certaines plates-formes de calcul et certains services. Chaque hiérarchie est déléguée du niveau supérieur ; il n'y a pas d'anonymat dans les noms de domaines. la messagerie électronique, HTTP, et les adresses SIP font tous référence aux noms de domaines.

Les numéros IP sont une fusion de deux espaces de noms, les noms des interfaces de réseautage d'un hôte et les noms des localisations ("fusion"' est le terme utilisé en statistiques pour parler de métriques qui sont fusionnées en une seule avec un gain d'indexation, mais une perte de valeur informationnelle). Les noms de localisations devraient être compris comme

notant des vecteurs de direction d'acheminement, c'est-à-dire, des informations utilisées pour livrer les paquets à leur destination.

Les numéros IP nomment des interfaces de réseautage, et normalement seulement quand l'interface est connectée au réseau. À l'origine, les numéros IP avaient une signification à long terme. Aujourd'hui, dans leur grande majorité, les interfaces utilisent des numéros IP éphémères et/ou non uniques. C'est-à-dire que chaque fois qu'une interface est connectée au réseau, il lui est alloué un numéro IP.

Dans l'Internet actuel, les couches de transport sont couplées aux adresses IP. Ni les unes ni les autres ne peuvent évoluer séparément. Les délibérations de l'IPng *(ng pour nouvelle génération)* ont été fortement structurées par la décision qu'un TCPng correspondant ne serait pas créé.

Il y a trois déficiences critiques des espaces de noms actuels. D'abord, le réadressage dynamique ne peut pas être géré directement. Ensuite, l'anonymat n'est pas fourni d'une manière cohérente et fiable. Enfin, l'authentification n'est pas fournie pour les systèmes et datagrammes. Ces trois déficiences surviennent parce que les plates-formes de calcul ne sont pas bien désignées avec les espaces de noms actuels.

4.1 Désir d'un espace de noms pour les plates-formes de calcul

Un espace de noms indépendant pour les plates-formes de calcul pourrait être utilisé dans les opérations de bout en bout indépendamment de l'évolution de la couche d'inter réseautage et à travers les nombreuses couches d'inter réseautage.

Cela pourrait prendre en charge un réadressage rapide de la couche d'inter réseautage à cause de la mobilité, du re rattachement, ou de la dénumérotation.

Si l'espace de noms pour les plates-formes de calcul se fonde sur une cryptographie à clé publique, il peut aussi fournir des services d'authentification. Si cet espace de noms est créé localement sans exiger d'enregistrement, il peut fournir l'anonymat.

Un tel espace de noms (pour plates-formes de calcul) et les noms dedans, devraient avoir les caractéristiques suivantes :

- L'espace de noms devrait être appliqué au "noyau" IP. Le noyau IP est le "composant" entre les applications et l'infrastructure de transport de paquets.

- L'espace de noms devrait complètement découpler la couche d'inter réseautage des couches supérieures. Les noms devraient remplacer toutes les occurrences d'adresses IP au sein des applications (comme le bloc de contrôle de transport (TCB, *Transport Control Block*)). Cela peut exiger des changements aux API actuelles. À long terme, il est probable que de nouvelles API seront nécessaires.

- L'introduction de l'espace de noms ne devrait pas rendre obligatoire une infrastructure administrative. Le déploiement doit venir du bas, dans un déploiement apparié.

- Les noms devraient avoir une représentation de longueur fixe, pour une inclusion facile dans les en-têtes de datagrammes et les interfaces existantes de programmation (par exemple, le TCB).

- L'utilisation de l'espace de noms devrait être possible dans les protocoles. Ceci est principalement une question de taille de paquet. Il y a aussi un souci de capacité de calcul dans cette disponibilité.

- Les collisions de noms devraient être évitées autant que possible. La mathématique du paradoxe de l'anniversaire peut être utilisée pour estimer les chances d'une collision dans une certaine population et espace de hachage. En général, pour un espace de hachage aléatoire de n bits, on s'attend à obtenir une collision après qu'approximativement 1,2*√(2**n) hachages ont été obtenus. Pour 64 bits, ce nombre est en gros de 4 milliards. Une taille de hachage de 64 bits peut être trop petite pour éviter des collisions dans une grande population ; par exemple, il y a 1 % de chances de collision dans une population de 640 M. Pour 100 bits (ou plus) on n'attend pas de collision avant qu'approximativement 2**50 (10 puissance 15) hachages aient été générés.

- Les noms devraient avoir une abstraction localisée qui puisse être utilisée dans les protocoles et API existants.

- Il doit être possible de créer localement les noms. Cela peut assurer l'anonymat au prix d'une résolvabilité rendue très difficile.

  * Parfois les noms peuvent contenir un composant de délégation. C'est le prix de la résolvabilité.

- L'espace de noms devrait fournir des services d'authentification.

- Les noms devraient être à longue durée, mais remplaçables à tout moment. Cela impacte les listes de contrôle d'accès ; des durées de vie courtes vont tendre à résulter en une maintenance de liste laxiste ou à exiger une infrastructure d'espace de noms pour un contrôle central des listes d'accès.

Dans ce document, un nouvel espace de noms approchant de ces idées est appelé espace de noms d'identité d'hôte. Utiliser des identités d'hôte exige sa propre couche de protocole, le protocole d'identité d'hôte, entre les couches d'inter réseautage et de transport. Les noms se fondent sur la cryptographie à clé publique pour fournir les services d'authentification. Conçu de façon appropriée, cela peut satisfaire toutes les exigences mentionnées ci-dessus.

5. Espace de noms Identité d'hôte

Un nom dans l'espace de noms d'identité d'hôte, un identifiant d'hôte (HI), représente un nom statistiquement unique au monde pour désigner tout système avec une pile IP. Cette identité est normalement associée, mais pas limitée, à une pile IP. Un système peut avoir plusieurs identités, certaines "bien connues", certaines non publiées ou "anonymes". Un système peut auto certifier sa propre identité, ou peut utiliser un authentifiant par un tiers comme la sécurité du DNS (DNSSEC) [RFC4033], "Pretty Good Privacy" (PGP), ou X.509 pour "notarier" l'affirmation d'identité. On s'attend à ce que les identifiants d'hôte soient initialement authentifiés avec DNSSEC et que toutes les mises en œuvre prennent en charge DNSSEC au minimum.

En théorie, tout nom qui peut prétendre être "statistiquement unique au monde" peut servir d'identifiant d'hôte. Cependant, de l'avis des auteurs, une clé publique d'une "paire de clés publiques" constitue le meilleur identifiant d'hôte. Comme il sera spécifié dans le protocole d'identité d'hôte, un identifiant d'hôte fondé sur une clé publique peut authentifier les paquets HIP et les protéger contre les attaques par interposition. Comme les datagrammes authentifiés sont obligatoires pour fournir la plus grande partir de la protection de HIP contre le déni de service, l'échange Diffie-Hellman dans HIP doit être authentifié. Donc, seuls les identifiants d'hôte à clé publique et les messages HIP authentifiés sont pris en charge en pratique. Dans le présent document, les formes non cryptographiques de HI et HIP sont présentées pour compléter la théorie de HI, mais elles ne devraient pas être mises en œuvre car elles pourraient produire de pires attaques de DoS que ce qu'a l'Internet sans identité d'hôte.

5.1 Identifiants d'hôte

L'identité d'hôte ajoute deux caractéristiques principales aux protocoles Internet. La première est un découplage des couches d'inter réseautage et de transport ; voir la Section 6. Ce découplage va permettre une évolution indépendante des deux couches. De plus, il peut fournir des services de bout en bout sur plusieurs domaines d'inter réseautage. La seconde caractéristique est l'authentification d'hôte. Parce que l'identifiant d'hôte est une clé publique, cette clé peut être utilisée pour l'authentification dans des protocoles de sécurité comme IPsec.

La seule structure complètement définie de l'identité d'hôte est celle d'une paire de clés publique/privée. Dans ce cas, l'identité d'hôte est référée par son composant public, la clé publique. Donc, le nom représentant une identité d'hôte dans l'espace de noms d'identité d'hôte, c'est-à-dire, l'identifiant d'hôte, est la clé publique. D'une certaine façon, la possession de la clé privée définit l'identité elle-même. Si la clé privée est possédée par plus d'un nœud, l'identité peut être considérée comme étant une identité répartie.

Architecturalement, toute autre convention de dénomination de l'Internet peut former une base utilisable pour les identifiants d'hôte. Cependant, des noms non cryptographiques ne devraient être utilisés que dans des situations de forte confiance/faible risque, c'est-à-dire, tout endroit où l'authentification de l'hôte n'est pas nécessaire (pas de risque d'hôte déguisé et pas d'utilisation de IPsec). Cependant, au moins pour les réseaux interconnectés s'étendant sur plusieurs domaines de fonctionnement, l'ensemble des environnements où le risque de déguisement d'hôte permis par un identifiant d'hôte non cryptographique est acceptable est l'ensemble nul. Donc, les documents HIP actuels ne spécifient pas comment utiliser d'autres types d'identifiants d'hôte que des clés publiques.

Les identités d'hôte réelles ne sont jamais directement utilisées dans un des protocoles de l'Internet. Les identifiants d'hôte (clés publiques) correspondants peuvent être mémorisés dans divers répertoires du DNS ou du protocole léger d'accès à un répertoire (LDAP, *Lightweight Directory Access Protocol*) comme identifié ailleurs dans le présent document, et ils sont passés dans l'échange de base HIP. Une étiquette d'identité d'hôte (HIT) est utilisée dans d'autres protocoles pour

représenter l'identité d'hôte. Une autre représentation des identités d'hôte, l'identifiant de portée locale (LSI, *Local Scope Identifier*) peut aussi être utilisé dans les protocoles et API.

5.2 Mémorisation des identifiants d'hôte dans le DNS

Les identifiants d'hôte publics devraient être mémorisés dans le DNS ; les identifiants d'hôte non publiés ne devraient être mémorisés nulle part (en dehors des hôtes communicants eux-mêmes). Le HI (public) est mémorisé dans un nouveau type d'enregistrement de ressource (RR, *Resource Record*) à définir. Ce type de RR sera vraisemblablement assez similaire au RR IPSECKEY [RFC4025].

Autrement, ou en plus de mémoriser les identifiants d'hôte dans le DNS, ils peuvent être mémorisés dans diverses sortes d'infrastructures de clé publique (PKI, *Public Key Infrastructure*). Cette pratique peut leur permettre d'être utilisés pour des besoins autres que la pure identification d'hôte.

5.3 Étiquette d'identité d'hôte (HIT)

Une étiquette d'identité d'hôte est une représentation sur 128 bits d'une identité d'hôte. Elle est créée en prenant un hachage cryptographique de l'identifiant d'hôte correspondant. Il y a deux avantages à utiliser un hachage par rapport à un identifiant d'hôte dans les protocoles. D'abord, sa longueur fixe rend plus facile le codage du protocole et aussi gère mieux le coût de la taille de paquet de cette technologie. Ensuite, cela présente l'identité dans un format cohérent pour le protocole indépendamment des algorithmes de chiffrement utilisés.

Dans les paquets HIP, les HIT identifient l'envoyeur et le receveur d'un paquet. Par conséquent, un HIT devrait être unique dans l'univers IP entier aussi longtemps qu'il est utilisé. Dans le cas extrêmement rare d'une seule transposition de HIT en plus d'une identité d'hôte, les identifiants d'hôte (clés publiques) vont faire la différence. Si il y a plus d'une clé publique pour un certain nœud, le HIT agit comme indication de la clé publique correcte à utiliser.

5.4 Identifiant de portée locale (LSI)

Un identifiant de portée locale (LSI, *Local Scope Identifier*) est une représentation localisée de 32 bits pour une identité d'hôte. L'objet d'un LSI est de faciliter l'utilisation des identités d'hôte dans les protocoles et API existants. L'avantage des LSI sur le HIT est sa taille ; son inconvénient est sa portée locale.

Exemples d'utilisation des LSI : l'adresse dans une commande FTP, et comme adresse dans un appel de prise. Donc, les LSI agissent comme un pont pour les identités d'hôte dans les protocoles et API fondés sur IPv4.

6. Architecture de la nouvelle pile

Une façon de caractériser l'identité d'hôte est de comparer la nouvelle architecture proposée à l'actuelle. Comme expliqué ci-dessus, les adresses IP peuvent être vues comme étant une fusion de vecteurs de direction d'acheminement et de noms d'interfaces. En utilisant la terminologie du rapport du groupe de recherches sur l'espace de noms de l'IRTF [NSRG] et, par exemple, le projet Internet non publié "Points d'extrémité et noms de points d'extrémité" [Chiappa] par Noel Chiappa, les adresses IP incorporent actuellement le double rôle de localisateurs et d'identifiant de point d'extrémité. C'est-à-dire que chaque adresse IP désigne une localisation topologique dans l'Internet, agissant par là comme un vecteur de direction d'acheminement, ou localisateur. En même temps, l'adresse IP désigne l'interface physique de réseau actuellement située au point de rattachement, agissant par là comme un nom de point d'extrémité.

Dans l'architecture HIP, les noms de point d'extrémité et les localisateurs sont séparés les uns des autres. Les adresses IP continuent d'agir comme des localisateurs. Les identifiants d'hôte prennent le rôle d'identifiants de point d'extrémité. Il est important de comprendre que les noms de point d'extrémité fondés sur les identités d'hôte sont légèrement différents des noms d'interface ; une identité d'hôte peut être simultanément accessible par plusieurs interfaces.

La différence entre les liens des entités logiques est illustrée par la Figure 1.

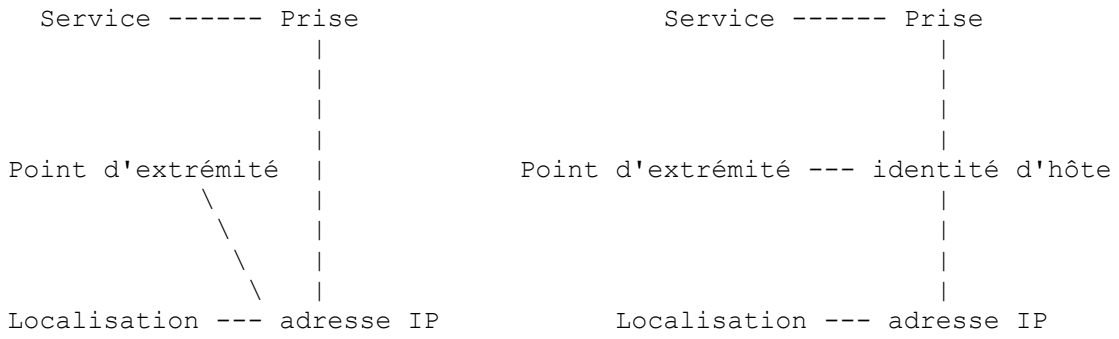

Figure 1

6.1 Associations de transport et points d'extrémité

Par son architecture, HIP assure un lien différent des protocoles de couche transport. Les associations de couche, c'est-à-dire, les connexions TCP et les associations UDP, ne sont plus liées aux adresses IP mais aux identités d'hôte.

Il est possible qu'un seul ordinateur physique héberge plusieurs points d'extrémité logiques. Avec HIP, chacun de ces points d'extrémité va avoir une identité d'hôte distincte. De plus, comme les associations de transport sont liées aux identités d'hôte, HIP assure la migration du processus et des grappes de serveurs. C'est-à-dire que si une identité d'hôte est déplacée d'un ordinateur physique à un autre, il est aussi possible de déplacer simultanément toutes les associations de transport sans les casser. De même, si il est possible de répartir le traitement d'une seule identité d'hôte sur plusieurs ordinateurs physiques, HIP assure des services fondés sur la grappe sans aucun changement chez le point d'extrémité client.

7. Mobilité d'hôte d'extrémité et multi rattachements

HIP découple le transport de la couche d'inter réseautage, et lie les associations de transport aux identités d'hôte (soit par le HIT, soit par le LSI). Par conséquent, HIP peut fournir un degré de mobilité d’inter réseautage et de multi rattachement à un faible coût d'infrastructure. La mobilité HIP inclut les changements d'adresse IP (via toute méthode) sur l'une ou l'autre partie. Donc, un système est considéré comme mobile si son adresse IP peut changer de façon dynamique pour n'importe quelle raison comme PPP, le protocole de configuration dynamique d'hôte (DHCP), des réallocations de préfixes IPv6, ou une retransposition de la traduction d'un appareil de traduction d'adresse réseau (NAT). De même, un système est considéré comme multi rattachements si il a plus d'une adresse IP mondialement acheminable en même temps. HIP relie les adresses IP, quand plusieurs adresses IP correspondent à la même identité d'hôte, et si une adresse devient inutilisable, ou si une adresse préférée devient disponible, les associations de transport existantes peuvent facilement être déplacées à une autre adresse.

Si un nœud se déplace alors qu'une communication est déjà en cours, les changements d'adresse sont assez directs. L'homologue du nœud mobile peut juste accepter un paquet HIP ou un paquet IPsec protégé en intégrité provenant de toute adresse et ignorer l'adresse de source. Cependant, comme expliqué au paragraphe 7.2, un nœud mobile doit envoyer un paquet de réadressage HIP pour informer l'homologue de la ou des nouvelles adresses, et l'homologue doit vérifier que le nœud mobile est accessible par ces adresses. Ceci est particulièrement utile pour les situations où le nœud homologue est en train d'envoyer périodiquement des données au nœud mobile (qui redémarre une connexion après la connexion initiale).

7.1 Mécanisme de rendez-vous

Faire un contact avec un nœud mobile est légèrement plus compliqué. Afin de démarrer l'échange HIP, le nœud initiateur doit savoir comment atteindre le nœud mobile. Bien que les nœuds HIP qui bougent de façon peu fréquente puissent utiliser le DNS dynamique [RFC2136] pour mettre à jour leurs informations d'accessibilité dans le DNS, un moyen de remplacement de l'utilisation du DNS de cette façon est d'utiliser un élément de la nouvelle infrastructure statique pour faciliter le rendez-vous entre les nœuds HIP.

Le nœud mobile garde l'infrastructure de rendez-vous continuellement à jour avec sa ou ses adresses IP actuelles. Les nœuds mobiles doivent faire confiance au mécanisme de rendez-vous pour tenir de façon appropriée leurs transpositions d''adresses HIT et IP.

Le mécanisme de rendez-vous est aussi nécessaire si les deux nœuds se trouvent changer leur adresse en même temps, soit parce que ils sont mobiles et se trouvent bouger au même moment, parce que l'un d'eux est hors ligne pendant un temps, soit pour quelque autre raison. Dans ce cas, les paquets HIP de réadressage vont se croiser dans le réseau et ne jamais atteindre le nœud homologue.

Un document séparé spécifiera les détails du mécanisme de rendez-vous HIP.

7.2 Protection contre les attaques d'inondation

Bien que l'idée d'informer des changements d'adresse par un simple envoi de paquets avec une nouvelle adresse de source paraisse séduisante, elle n'est pas assez sûre. C'est-à-dire que même si HIP ne s'appuie en rien sur l'adresse de source (une fois que l'échange de base a été achevé) il apparaît qu'il est nécessaire de vérifier l'accessibilité d'un nœud mobile à la nouvelle adresse avant de réellement envoyer de plus grosses quantités de trafic à la nouvelle adresse.

Accepter aveuglément de nouvelles adresses conduirait potentiellement à des attaques de DoS par inondation contre des tiers [RFC4225]. Dans une attaque d'inondation répartie, un attaquant ouvre des connexions HIP à gros volume avec un grand nombre d'hôtes (en utilisant des HI non publiés) et ensuite prétend à tous ces hôtes qu'il est passé à l'adresse IP du nœud cible. Si les hôtes homologues se trouvent simplement accepter le mouvement, le résultat va être une inondation de paquets à l'adresse du nœud cible. Pour clore cette attaque, HIP inclut un mécanisme de vérification d'adresse où l'accessibilité d'un nœud est vérifiée séparément à chaque adresse avant d'utiliser l'adresse pour de plus grosses quantités de trafic.

Chaque fois que HIP est utilisé entre deux hôtes qui ont une pleine confiance mutuelle, les hôtes peuvent facultativement décider de sauter les vérifications d'adresses. Cependant, une telle optimisation de performances doit être restreinte aux homologues qui sont connus pour être de confiance et capables de se protéger contre les logiciels malveillants.

8. HIP et IPsec

La façon préférée de mettre en œuvre HIP est d'utiliser IPsec pour porter le trafic réel de données. À ce jour, la seule méthode complètement définie est d'utiliser l'encapsulation de charge utile de sécurité (ESP, *Encapsulating Security Payload*) IPsec pour porter les paquets de données. À l'avenir, d'autres façons de transporter les données de charge utile pourront être développées, incluant celles qui n'utilisent pas de protection cryptographique.

En pratique, l'échange fondé sur HIP utilise les identifiants d'hôte cryptographiques pour établir une paire d'associations de sécurité ESP pour activer ESP de bout en bout. Ceci est mis en œuvre d'une façon qui peut couvrir les domaines d'adressage.

Bien qu'il soit possible, au moins en théorie, d'utiliser des protocoles de chiffrement existants comme IKEv2 avec des identifiants d'hôte, pour établir les associations de sécurité nécessaires, HIP définit un nouveau protocole. Il y a un certain nombre de raisons historiques pour cela, et il y a aussi quelques raisons architecturales. D'abord, IKE et IKEv2 n'ont pas été conçus en visant les boîtiers de médiation. Comme l'ajout d'une nouvelle couche de désignation permet potentiellement d'ajouter une nouvelle couche de transmission (voir la Section 9) il est très important que les protocoles HIP soient bien adaptés à un environnement de boîtiers de médiation.

Ensuite, d'un point de vue conceptuel, l'indice de paramètre de sécurité (SPI, *Security Parameter Index*) dans IPsec ESP fournit une simple compression des HIT. Cela exige des associations de sécurité par paire de HIT (et de SPI) et une diminution de la granularité de la politique sur les autres protocole de gestion de clés, comme IKE et IKEv2. En particulier, les réflexions actuelles sont limitées à une situation dans laquelle, conceptuellement, il y a seulement une paire de SA entre toute paire de HIT. En d'autres termes, d'un point de vue architectural, HIP prend seulement en charge des associations de sécurité d'hôte à hôte (ou de point d'extrémité à point d'extrémité). Si deux hôtes ont besoin de plus de paires de SA parallèles, elles devraient utiliser des HIT séparées pour cela. Cependant, de futures extensions de HIP pourront assurer plus de granularité et la création de plusieurs SA ESP entre une paire de HIT.

Comme HIP est conçu pour l'usage d'hôtes, et non pour des passerelles ou ce qu'on appelle des mises en œuvre "prises dans le réseau" (BITW, *Bump-in-the-Wire*) seul le mode transport est pris en charge. Une paire de SA ESP est indexée par les SPI et les deux HIT (car un système peut avoir plus d'une HIT). Les SA n'ont pas besoin d'être liées aux adresses IP ; tout le contrôle interne de la SA est fait par les HIT. Donc, un hôte peut aisément changer son adresse en utilisant le réadressage IP mobile, DHCP, PPP, ou IPv6 et conserver quand même les SA.

Comme les transports sont liés à la SA (via un LSI ou une HIT) tout transport actif est aussi conservé. Donc, les conditions du monde réel comme la perte d'une connexion PPP et son rétablissement ou un transfert inter-cellulaire mobile ne vont pas exiger une négociation HIP ou une interruption des services de transport [HostNAT].

Comme HIP ne négocie aucune durée de vie de SA, toutes les durées de vie sont du ressort de la politique locale. Les seules durées de vie qu'une mise en œuvre HIP doit prendre en charge sont le retour à zéro des numéros de séquence (pour la protection contre la répétition) et la fin de temporisation de SA. Une SA arrive en fin de temporisation si aucun paquet n'est reçu en utilisant cette SA. Les mises en œuvre peuvent prendre en charge les durées de vie des diverses transformations ESP.

9. HIP et les NAT

Passer des paquets entre différents domaines d'adressage IP exige de changer les adresses IP dans l'en-tête de paquet. Cela peut arriver, par exemple, quand un paquet est passé entre l'Internet public et un espace d'adresses privé, ou entre des réseaux IPv4 et IPv6. La traduction d'adresse est généralement mise en œuvre comme traduction d'adresse réseau (NAT) [RFC3022] ou traduction de protocole NAT (NAT-PT) [RFC2766].

Dans un environnement de réseau où l'identification se fonde sur les adresses IP, identifier les nœuds communicants est difficile quand un NAT est utilisé. Avec HIP, les points d'extrémité de la couche transport sont liés aux identités d'hôte. Donc, une connexion entre deux hôtes peut traverser de nombreuses frontières de domaines d'adressage. Les adresses IP ne sont utilisées que pour les besoins de l'acheminement ; elles peuvent être changées librement durant la traversée de paquet.

Pour un flux fondé sur HIP, un système de NAT ou NAT-PT à capacité HIP suit à la trace la transposition des HIT, et des SPI IPsec correspondants, en une adresse IP. Le système de NAT doit apprendre les transpositions des HIT et des SPI en adresses IP. De nombreux HIT (et SPI) peuvent se transposer en une seule adresse IP sur un NAT, simplifiant les connexions sur les interfaces de NAT pauvres en adresses. Le NAT peut obtenir une grande partie de ses connaissances des paquets HIP eux-mêmes ; cependant, une certaine configuration de NAT peut être nécessaire.

Les systèmes de NAT ne peuvent pas toucher aux datagrammes au sein de l'enveloppe IPsec ; donc, la traduction d'adresse spécifique d'application doit être faite dans les systèmes d'extrémité. HIP fournit le "NAT réparti", et utilise la HIT ou le LSI comme un bouche-trou pour les adresses IP incorporées.

9.1 HIP et sommes de contrôle TCP

Il n'y a pas de moyen pour un hôte de savoir si une des adresses IP dans un en-tête IP est l'adresse utilisée pour calculer la somme de contrôle TCP. C'est-à-dire qu'il n'est pas faisable de calculer la somme de contrôle TCP en utilisant les adresses IP réelles dans le pseudo en-tête ; les adresses reçues dans le paquet entrant ne sont pas nécessairement les mêmes que celles qui étaient chez l'hôte envoyeur. De plus, il n'est pas possible de recalculer les sommes de contrôle de couche supérieure dans le système NAT/NAT-PT, car le trafic est protégé par IPsec. Par conséquent, les sommes de contrôle TCP et UDP sont calculées en utilisant les HIT à la place des adresses IP dans le pseudo en-tête. De plus, seul le format de pseudo en-tête IPv6 est utilisé. Cela assure la traduction de protocole IPv4/IPv6.

10. Diffusion groupée

À la fin 2003, il n'y avait pour ainsi dire pas de réflexions concrètes sur la façon dont HIP pourrait affecter la diffusion groupée à la couche IP ou application.

11. Politiques HIP

Un certain nombre de variables qui vont influencer les échanges HIP doivent être prises en charge par chaque hôte. Toutes les mises en œuvre de HIP devraient prendre en charge au moins deux HI, une à publier dans le DNS et une non publiée pour l'usage anonyme. Bien que les HI non publiées soient rarement utilisées comme HI de répondant, elles vont probablement être courantes pour les initiateurs. La prise en charge de plusieurs HI est recommandée.

De nombreux initiateurs vont vouloir utiliser une HI différente pour les différents répondants. Les mises en œuvre devraient fournir une politique d'initiateur HIT à répondant HIT. Cette politique devrait aussi inclure les transformations préférées et les durées de vie locales.

Les répondants vont avoir besoin d'une politique similaire, décrivant les hôtes auxquels il est permis de participer aux échanges HIP, et les transformations et durées de vie locales préférées.

12. Avantages de HIP

Au début, le protocole de couche réseau (c'est-à-dire, IP) avait les quatre invariants "classiques" suivants :
- o Non mutable : l'adresse envoyée est l'adresse reçue.
- o Non mobile : l'adresse ne change pas durant le cours d'une "association".
- o Réversible : un en-tête de retour peut toujours être formé en inversant les adresses de source et de destination.
- o Omniscient : chaque hôte sait quelle adresse un hôte partenaire peut utiliser pour lui envoyer des paquets.

En fait, le quatrième peut être inféré de 1 et 3, mais il vaut de le mentionner pour les raisons qui suivent.

Dans le monde "post-classique" actuel, on essaye intentionnellement de se débarrasser du second invariant (à la fois pour la mobilité et pour le multi rattachements) et on a été forcé d'abandonner le premier et le quatrième. IP spécifique du domaine [RFC3102] est une tentative de mettre sur pied le quatrième invariant sans le premier. IPv6 est une tentative de réinstaller le premier invariant.

Peu de systèmes sur l'Internet ont des noms DNS qui soient significatifs. C'est-à-dire, si ils ont un nom de domaine pleinement qualifié (FQDN) ce nom appartient normalement à un appareil de NAT ou à un serveur de numérotation, et n'identifie pas réellement le système lui-même mais sa connectivité actuelle. Les FQDN (et leurs extensions comme noms de messagerie) sont des noms de couche d'application, qui plus fréquemment désignent des services plutôt qu'un système particulier. C'est pourquoi de nombreux systèmes sur l'Internet ne sont pas enregistrés dans le DNS; ils n'ont pas de services qui intéressent les autres hôtes de l'Internet.

Les noms DNS sont des références aux adresses IP. Cela montre seulement les inter relations des couches de réseautage et d'application. Le DNS, comme seule base de données répartie déployée dans l'Internet, est aussi le dépositaire des autres espaces de noms, due en partie aux enregistrements de clés spécifiques de DNSSEC et des applications. Bien que chaque espace de noms puisse être étendu (IP avec v6, DNS avec les enregistrements "KEY") aucun ne peut de façon adéquate fournir l'authentification d'hôte ou agir comme séparation entre les couches d'inter réseautage et de transport.

L'espace de noms "identité d'hôte" (HI) bouche un trou important entre les espaces de noms IP et DNS. Une chose intéressante sur la HI est qu'elle permet en fait d'abandonner tout sauf le troisième invariant de couche réseau. C'est-à-dire que tant que les adresses de source et de destination dans le protocole de couche réseau sont réversibles, tout fonctionne bien parce que HIP prend soin de l'identification de l'hôte, et la réversibilité permet de faire revenir un paquet à l'hôte partenaire. On ne se soucie pas que l'adresse de couche réseau change dans le transit (mutable), et on ne se soucie pas de quelle adresse de couche réseau le partenaire se sert (non omniscient).

12.1 Réponses de HIP aux questions du NSRG

Le groupe de recherche de l'espace de noms de l'IRTF a posé un certain nombre de questions d'évaluation dans son rapport [NSRG]. Ce paragraphe fournit les réponses à ces questions.

1. Comment un nom de pile va t-il améliorer le fonctionnement global de l'Internet ?
   HIP découple la couche d'inter réseautage de la couche transport, permettant à chacune d'évoluer séparément. Le découplage rend plus faciles la mobilité de l'hôte d'extrémité et le multi rattachements, aussi à travers les réseaux IPv4 et IPv6. Les HI rendent plus facile le renumérotage de réseau, et elles rendent aussi plus faciles à mettre en œuvre la migration de processus et les serveurs en grappes. De plus, étant cryptographiques par nature, elles fournissent une base pour résoudre les problèmes de sécurité relatifs à la mobilité et au multi rattachements de l'hôte d'extrémité.

2. À quoi ressemble un nom de pile ?
   Une HI est une clé publique cryptographique. Cependant, au lieu d'utiliser les clés directement, la plupart des protocoles utilisent un hachage de taille fixe de la clé publique.

3 Quelle est sa durée de vie ?

HIP fournit des identifiants d'hôte à la fois stables et temporaires. Les HI stables sont normalement de longue durée de vie, de plusieurs années. La durée de vie des HI temporaires dépend du temps pendant lequel les connexions et applications de couche supérieure en ont besoin, et peut aller de quelques secondes à des années.

4. Qu'est ce qui vit dans la pile ?
   Les HI vivent entre les couches transport et inter réseautage.

5. Comment est il utilisé sur les points d'extrémité ?
   Les identifiants d'hôte peuvent être utilisés directement ou indirectement (sous forme de HIT ou de LSI) par les applications quand elles accèdent aux services réseau. De plus, les identifiants d'hôte, comme clés publiques, sont utilisés dans le protocole d'accord de clé incorporé, appelé échange de base HIP, pour authentifier mutuellement les hôtes.

6. Quelle infrastructure administrative est nécessaire pour le prendre en charge ?
   Dans certains environnements, il est possible d'utiliser HIP de façon opportuniste, sans aucune infrastructure. Cependant, pour tirer le meilleur parti de HIP, les HI doivent être mémorisés dans le DNS ou une PKI, et un nouveau mécanisme de rendez-vous est nécessaire. Un tel mécanisme nouveau de rendez-vous peut devoir imposer le déploiement d'une nouvelle infrastructure.

7. Si on ajoute une couche supplémentaire, cela rendra t-il inutile la liste d'adresses dans le protocole de transmission de commandes de flux (SCTP, *Stream Control Transmission Protocol*) ? oui.

8. Quels avantages de sécurité supplémentaires offrira un nouveau schéma de désignations ?
   HIP réduit la dépendance aux adresses IP, rendant plus faciles à résoudre les problèmes de propriété d'adresses [Nikander]. En pratique, HIP fournit la sécurité pour la mobilité et le multi rattachements de l'hôte d'extrémité. De plus, comme les identifiants d'hôte HIP sont des clés publiques, l'infrastructure standard de certificat de clé publique peut être appliquée par dessus HIP.

9. Que pourrait être le mécanisme de résolution, ou quelles caractéristiques d'un mécanisme de résolution seront exigées ?
   Pour la plupart des besoins, une approche où les noms DNS sont résolus simultanément aux HI et adresses IP est suffisant. Cependant, si il devient nécessaire de résoudre les HI en adresses IP ou de revenir aux noms DNS, une infrastructure de résolution plate est nécessaire. Une telle infrastructure pourrait se fonder sur les idées de tableaux de hachage répartis, mais exigerait des développements et déploiements nouveaux significatifs.

13. Considérations sur la sécurité

HIP tire parti du paradigme de la nouvelle identité d'hôte pour fournir une authentification sûre des hôtes et pour fournir un échange de clés rapide pour IPsec. HIP tente aussi de limiter l'exposition de l'hôte aux diverses attaques de déni de service (DoS) et d'interposition (MitM, *Man-in-the-Middle*). Ce faisant, HIP lui-même est soumis à ses propres attaques de DoS et MitM qui pourraient potentiellement être plus dommageables à la capacité de l'hôte de conduire ses affaires comme d'habitude.

Les attaques de DoS par épuisement des ressources tirent parti du coût de l'établissement d'un état pour un protocole chez le répondant par rapport à son "bon marché" chez l'initiateur. HIP permet à un répondant d'augmenter le coût du démarrage de l'état chez l'initiateur et fait un effort pour réduire le coût chez le répondant. Ceci est fait par le démarrage de l'échange authentifié Diffie-Hellman par le répondant au lieu de l'initiateur, faisant un échange de base HIP long de quatre paquets. Il y a plus de détails sur ce processus dans le protocole d'identité d'hôte (RFC7401).

HIP prend facultativement en charge une négociation opportuniste. C'est-à-dire que si l'hôte reçoit un début de transport sans une négociation HIP, il peut tenter de forcer un échange HIP avant d'accepter la connexion. Ceci a un potentiel d'attaques de DoS contre les deux hôtes. Si la méthode de forcer le début de HIP est coûteuse pour les deux hôtes, l’attaquant a seulement besoin de contrefaire un SYN TCP. Cela va engager les deux systèmes dans des opérations coûteuses. HIP évite cette attaque en faisant que le répondant envoie un simple paquet HIP qu'il peut pré construire. Comme ce paquet est fixe et facilement répété, l'initiateur n'y réagit que si il a juste commencé une connexion avec le répondant.

Il est difficile de se défendre contre les attaques de MitM sans une authentification par un tiers. Un interposé habile pourrait facilement traiter toutes les parties de l'échange de base HIP, mais HIP fournit indirectement la protection suivante contre une attaque de MitM. Si la HI du répondant est restituée d'une zone signée du DNS ou sécurisée par quelque autre moyen,

l'initiateur peut utiliser cela pour authentifier les paquets HIP signés. De même, si la HI de l'initiateur est dans une zone sûre du DNS, le répondant peut la restituer et valider les paquets HIP signés. Cependant, comme un initiateur peut choisir d'utiliser une HI non publiée, il risque une attaque de MitM en connaissance de cause. Le répondant peut choisir de ne pas accepter un échange HIP avec un initiateur qui utilise une HI inconnue.

Dans HIP, l'association de sécurité pour IPsec est indexée par le SPI ; l'adresse de source est toujours ignorée, et l'adresse de destination peut aussi être ignorée. Donc, la charge utile de sécurité encapsulée IPsec à capacité HIP est indépendante de l'adresse IP. Il peut sembler que cela rende les choses plus faciles à un attaquant, mais ESP avec la protection contre la répétition est déjà aussi bien protégé que possible, et la suppression de l'adresse IP comme vérification ne va pas augmenter l'exposition de ESP IPsec aux attaques de DoS.

Comme tous les hôtes ne vont pas prendre en charge HIP, les messages ICMPv4 "Destination injoignable, protocole inaccessible" et ICMPv6 "Problème de paramètre, prochain en-tête non reconnu" sont à prévoir et présentent une attaque de déni de service. Contre un initiateur, l'attaque va ressembler à un répondant qui ne prend pas HIP en charge, mais peu après avoir reçu le message ICMP, l'initiateur va recevoir un paquet HIP valide. Donc, pour se protéger contre cette attaque, un initiateur ne devrait pas réagir à un message ICMP avant qu'un délai raisonnable soit écoulé, lui permettant d'obtenir le vrai paquet HIP du répondant. Une attaque similaire contre le répondant est plus inquiétante.

Une autre attaque de MitM est de simuler le rejet administratif d'un répondant d'une initiation HIP. C'est un simple message ICMP "Destination injoignable, interdiction administrative". Un paquet HIP n'est pas utilisé parce qu'il devrait avoir un contenu unique, et donc difficile à générer, résultant en une autre attaque de déni de service, ou être juste aussi contrefait que le message ICMP. Comme dans le cas précédant, la défense contre cette attaque est que l'initiateur attende un délai raisonnable pour obtenir un paquet HIP valide. Si cela n'arrive pas, l'initiateur doit alors supposer que le message ICMP est valide. Comme c'est le seul point dans l'échange HIP de base où ce message ICMP est approprié, il peut être ignoré à tout autre moment de l'échange.

13.1 Utilisation de HIT dans les ACL

On prévoit que les HIT seront utilisées dans les listes de contrôle d'accès (ACL, MitM). De futurs pare-feu peuvent utiliser les HIT pour contrôler les entrées et sorties des réseaux, avec un niveau d'assurance difficile à réaliser aujourd'hui. Comme exposé à la Section 8, une fois qu'une session HIP a été établie, la valeur du SPI dans un paquet IPsec peut être utilisée comme indice, indiquant les HIT. En pratique, le pare-feu peut inspecter les paquets HIP pour apprendre les liens entre les HIT, les valeurs de SPI, et les adresses IP. Il peut même explicitement contrôler l'utilisation de IPsec, en ouvrant dynamiquement ESP IPsec pour seulement des valeurs de SPI et adresses IP spécifiques. Les signatures dans les paquets HIP permettent à un pare-feu de s'assurer que l'échange HIP se produit bien entre deux hôtes connus. Cela peut augmenter la sécurité du pare-feu.

Il y a eu un mauvaise expérience considérable avec des ACL réparties qui contiennent des matériaux en rapport avec des clés publiques, par exemple, avec le protocole Secure SHell (SSH). Si le possesseur d'une clé a besoin de la révoquer pour une raison quelconque, la tâche de trouver toutes les localisations où la clé est détenue dans une ACL peut être impossible. Si la raison de la révocation est due à un vol de la clé privée, ce peut être un problème sérieux.

Un hôte peut garder trace de tous ses partenaires qui peuvent utiliser sa HIT dans une ACL en enregistrant toutes les HIT distantes. Il devrait être seulement nécessaire d'enregistrer les hôtes répondants. Avec ces informations, l'hôte peut notifier aux divers hôtes les changements de la HIT. Il n'a pas été tenté de développer une méthode sûre pour produire l'avis de révocation de HIT.

Les NAT à capacité HIP, sont cependant par conception transparents aux systèmes à capacité HIP. Donc, l'hôte peut trouver difficile de notifier à un NAT qu'il utilise une HIT dans une ACL. Comme la plupart des systèmes connaissent les NAT pour leur réseau, il devrait y avoir un processus pour notifier à ces NAT le changement de la HIT. Ceci est obligatoire pour les systèmes qui fonctionnent comme répondants derrière un NAT. Dans une veine similaire, si un hôte est notifié d'un changement dans une HIT d'un initiateur, il devrait le notifier à son NAT. De cette manière, les NAT vont être mis à jour du changement de HIT.

13.2 Considérations non de sécurité

La définition de l'identifiant d'hôte déclare que la HI n'a pas besoin d'être une clé publique. Cela implique que la HI pourrait être n'importe quelle valeur ; par exemple, un FQDN. Le présent document ne décrit pas comment prendre en charge une telle HI non cryptographique. Une HI non cryptographique offrirait quand même les services de HIT ou LSI pour la traversée de NAT. Il serait possible de porter les HIT dans des paquets HIP qui n’auraient ni confidentialité ni

authentification. Comme un tel mode offrirait si peu de fonctionnalités supplémentaires pour un tel ajout au noyau IP qu'il n'a pas été défini. Étant donné le peu de cryptographie de clé publique que HIP exige, HIP ne devrait être mis en œuvre que en utilisant des identités d'hôte à clé publique.

Si on désire utiliser HIP dans une situation de faible sécurité où les calculs de clé publique sont considérés comme coûteux, HIP peut être utilisé avec des clés Diffie-Hellman et d'identité d'hôte très courtes. Une telle utilisation rend les hôtes participants vulnérables aux attaques de MitM et de capture de connexion. Cependant, elle ne cause pas de danger d'inondation, car le mécanisme de vérification d'adresse s'appuie sur le système d'acheminement et non sur la force du chiffrement.

14. Remerciements

Pour les personnes historiquement impliquées dans les premières étapes de HIP, voir la section Remerciements de la spécification du protocole d'identité d'hôte (RFC 7401).

Durant les dernières étapes de ce document, quand le relais de l'édition a été transféré à Pekka Nikander, les commentateurs des premières mises en œuvre et d'autres, incluant Jari Arkko, Tom Henderson, Petri Jokela, Miika Komu, Mika Kousa, Andrew McGregor, Jan Melen, Tim Shepard, Jukka Ylitalo, et Jorma Wall, ont été précieux. Finalement, Lars Eggert, Spencer Dawkins, et Dave Crocker ont fourni de précieux apports durant les stades finaux de la publication, dont la plupart ont été incorporés mais dont certains ont été ignorés par les auteurs afin de ne pas retarder la publication du document.

15. Références pour information

[Chiappa] Chiappa, J., "Endpoints and Endpoint Names: A Proposed Enhancement to the Internet Architecture", URL http://users.exis.net/~jnc/tech/endpoints.txt, 1999.

[HostNAT] Bellovin, S., "EIDs, IPsec, and HostNAT", in Proceedings of the 41st IETF, Los Angeles, CA, mars 1998.

[Nikander] Nikander, P., "Denial-of-Service, Address Ownership, et Early Authentication in the IPv6 World", dans Security Protocols, 9th International Workshop, Cambridge, UK, 25-27 avril 2001, LNCS 2467, pp. 12-26, Springer, 2002.

[NSRG] Lear, E. and R. Droms, "What's In A Name: Thoughts from the NSRG", Travail en cours, septembre 2003.

[RFC2136] P. Vixie, S. Thomson, Y. Rekhter et J. Bound, "Mises à jour dynamiques dans le système de noms de domaine (DNS UPDATE)", avril 1997.

[RFC2766] G. Tsirtsis, P. Srisuresh, "Traduction d'adresse réseau – traduction de protocole (NAT-PT)", février 2000. (*Obsolète, voir* RFC4966) (*MàJ par* RFC3152) *(Historique)*

[RFC3022] P. Srisuresh, K. Egevang, "Traducteur d'adresse réseau IP traditionnel", janvier 2001. *(Information)*

[RFC3102] M. Borella et autres, "IP spécifique de domaine : le cadre", octobre 2001. *(Expérimentale)*

[RFC4025] M. Richardson, "Méthode pour mémoriser le matériel de clés IPsec dans le DNS", mars 2005. *(P.S.)*

[RFC4033] R. Arends, et autres, "Introduction et exigences pour la sécurité du DNS", mars 2005.

[RFC4034] R. Arends et autres, "Enregistrements de ressources pour les extensions de sécurité au DNS", mars 2005.

[RFC4035] R. Arends et autres, "Modifications du protocole pour les extensions de sécurité du DNS", mars 2005. *(P.S. ; MàJ par* RFC8198

[RFC4225] P. Nikander et autres, "Fondements des concepts de sécurité de l'optimisation de l'acheminement d'IPv6 mobile", décembre 2005. *(Information)*

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

RFC5996)

Adresse des auteurs

Robert Moskowitz
ICSAlabs, a Division of Cybertrust Corporation
1000 Bent Creek Blvd, Suite 200
Mechanicsburg, PA
USA
mél : rgm@icsalabs.com

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

Déclaration complète de droits de reproduction

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