Groupe de travail Réseau
Request for Comments : 4218
Catégorie : Information
Traduction Claude Brière de L'Isle

E. Nordmark, Sun Microsystems
T. Li
octobre 2005

Menaces relatives aux solutions de multi rattachements IPv6

Résumét
Le présent document fait la liste des menaces sur la sécurité relatives au multi-rattachements IPv6. Les multi-rattachements peuvent introduire de nouvelles opportunités de rediriger des paquets sur des adresses IP différentes, non prévues.

L'intention est de regarder comment des solutions de multi-rattachement IPv6 pourraient rendre l'Internet moins sûr ; on examine les menaces inhérentes à toutes les solutions de multi-rattachements IPv6 plutôt que d'étudier une solution spécifique proposée. Les menaces dans ce document s'appuient sur les menaces découvertes et discutées au titre du travail sur IPv6 mobile.

Table des matières

1. Introduction....2
1.1 Hypothèses....2
1.2 Authentification, autorisation, et possession de l'identifiant....3
2. Terminologie....3
3. Hypothèses et attaques d'aujourd'hui....4
3.1 Hypothèses d'application....4
3.2 Attaques de redirection d'aujourd'hui....5
3.3 Attaques d'injection de paquet d'aujourd'hui....5
3.4 Attaques d'inondation d'aujourd'hui....6
3.5 Confidentialité de l'adresse aujourd'hui....7
4. Nouvelles attaques potentielles....8
4.1 Causer l'envoi des paquets à l'attaquant....8
4.2 Causer l'envoi des paquets à un trou noir....9
4.3 Attaques de déni de service par un tiers....9
4.4 Acceptation de paquets provenant de localisateurs inconnus....11
4.5 Nouvelles considérations de confidentialité....11
5. Granularité de redirection....11
6. Implications de mouvement ?....12
7. Autres problèmes de sécurité....13
8. Considérations sur la sécurité....14
9. Remerciements....14
10. Références pour information....14
Appendice A. Analyse de la sécurité....15
Adresse des auteurs....17
Déclaration complète de droits de reproduction....17

1. Introduction

Le but du travail sur le multi-rattachement IPv6 est de permettre à un site de tirer parti de plusieurs rattachements à l'Internet mondial, sans avoir une entrée spécifique pour le site visible dans le tableau d'acheminement mondial. Spécifiquement, une solution devrait permettre aux hôtes d'utiliser plusieurs rattachements en parallèle, ou de commuter de façon dynamique entre ces points de rattachement en cas de défaillance, sans impact sur les protocoles de couche de

transport et d'application.

Au plus haut niveau, les problèmes concernant la possibilité d'un tel "re-rattachement" des flux de paquets peuvent être appelées des "attaques de redirection" ; la capacité de causer l'envoi de paquets à un endroit qui n'est pas lié à la notion d'homologue du protocole de couche de transport et/ou application. Ces attaques font peser des menaces sur la confidentialité, l'intégrité, et la disponibilité. C'est-à-dire qu'un attaquant pourrait apprendre le contenu d'un flux particulier en le redirigeant sur un endroit où l'attaquant a un enregistreur de paquets. Si, au lieu d'un enregistreur, l'attaquant change les paquets et les envoie ensuite à leur destination ultime, l'intégrité du flux de données va être compromise. Finalement, l'attaquant peut simplement utiliser la redirection d'un flux comme attaque de déni de service.

Le présent document a été développé en considération de solutions de multi-rattachements construites autour d'une séparation de l'identité de réseau et de la localisation de réseau, que cette séparation implique ou non l'introduction d'un nouvel espace de noms d'identifiants séparé. Cependant, cette séparation n'est pas une exigence pour toutes les menaces, de sorte que cette taxonomie peut aussi s'appliquer à d'autres approches. Le présent document n'est pas destiné à examiner une seule solution proposée. Il est plutôt destiné à aider la discussion et l'évaluation de solutions proposées. En cataloguant les menaces connues, on peut aider à assurer que toutes les propositions traitent de toutes les menaces disponibles.

N'analysant pas une solution particulière, le présent document est naturellement incomplet. Une solution réelle devrait être analysée au titre de sa propre analyse de menaces, en particulier dans les domaines suivants :

1) Si la solution fait une séparation entre localisateurs et identifiants, alors la plupart des mécanismes de sécurité d'application devraient être liés à l'identifiant, et pas au localisateur. Donc, des travaux vont être nécessaires pour comprendre comment les attaques sur le mécanisme d'identifiant affecte la sécurité, en particulier des attaques sur le mécanisme qui vont lier les localisateurs aux identifiants.

2) Comment la solution applique t-elle le multi-rattachements à la diffusion groupée IP ? Selon la façon dont cela est fait, il pourrait y avoir des menaces spécifiques relatives à la diffusion groupée qu'il faudrait comprendre. Le présent document ne discute aucune menace spécifique de la diffusion groupée.

3) Les protocoles de transport sans connexion ont probablement besoin de plus d'attention. Ils sont déjà difficiles à sécuriser, même sans séparation localisateur/identifiant.

1.1 Hypothèses

Cette analyse de menaces ne suppose pas que la sécurité a été appliquée à d'autres parties de l'Internet relevant de la sécurité, comme le DNS et les protocoles d'acheminement ; mais elle suppose que, à un moment donné, au moins les parties de l'Internet vont fonctionner avec la sécurité pour une telle infrastructure de clés. Avec cette hypothèse, il devient alors important qu'une solution de multi-rattachements ne devienne pas, à ce moment, le maillon faible. C'est le cas même si, par exemple, un DNS non sûr pourrait être aujourd'hui, le maillon faible.

Le présent document ne suppose pas que les protocoles d'application sont protégés aujourd'hui ou dans le futur par une forte sécurité. Cependant, il est toujours utile de supposer que les protocoles d'application qui veillent sur l'intégrité et/ou la confidentialité appliquent les mesures de sécurité de bout en bout pertinentes, comme IPsec, TLS, et/ou la sécurité de couche d'application.

Dans un souci de simplicité, le présent document suppose qu'un attaquant sur le chemin peut voir les paquets, modifier les paquets et les envoyer, et bloquer la livraison des paquets. C'est une simplification parce que il pourrait exister des moyens (par exemple, en surveillant les capacités dans les commutateurs) qui permettent à des utilisateurs authentifiés et autorisés d'observer les paquets sans être capables d'envoyer ou bloquer les paquets.

Dans certains cas, il pourrait y avoir un sens à la distinction entre des attaquants dans le chemin, qui peuvent surveiller les paquets et peut-être aussi injecter des paquets, sans être capables de bloquer le passage des paquets.

Les attaquants dans le chemin qui ont seulement besoin de surveiller peuvent avoir de la chance et trouver un Ethernet non commuté dans le chemin, ou utiliser un couplage capacitif ou inductif pour écouter sur un fil de cuivre. Mais si l'attaquant est sur un Ethernet qui est sur le chemin, qu'il soit commuté ou non, l'attaquant peut aussi employer l'usurpation du protocole de résolution d'adresse/découverte de voisin (ARP/ND, *Address Resolution Protocol/Neighbor Discovery*) pour obtenir l'accès au flux de paquets qui permet aussi le blocage. De même, si l'attaquant a accès au réseau, il peut aussi placer un appareil sur le réseau pour bloquer. D'autres attaques en chemin vont être celles qui obtiennent le contrôle d'un routeur ou d'un commutateur (ou obtiennent le contrôle d'un des points d'extrémité) et très probablement cela va aussi permettre le

blocage.

Ainsi le cas le plus fort actuellement connu où la surveillance est plus facile que le blocage, est quand des commutateurs et des routeurs ont des capacités de surveillance (de la gestion du réseau ou pour des interceptions légales) où un attaquant pourrait être capable d'outrepasser les vérifications d'authentification et d'autorisation de ces capacités. Cependant, le présent document fait l'hypothèse simplificatrice de traiter tous les attaquants dans le chemin de la même façon en supposant qu'un tel attaquant peut surveiller, injecter, et bloquer les paquets. Une analyse de sécurité d'une proposition particulière peut bénéficier de ne pas faire cette hypothèse, et chercher comment les attaquants dans le chemin avec des capacités différentes peuvent générer des attaques différentes peut-être absentes de l'Internet d'aujourd'hui.

Le document suppose qu'un attaquant hors chemin ne peut ni voir les paquets entre les homologues (pour lesquels il n'est pas sur le chemin) ni bloquer leur livraison. Les attaquants hors chemin peuvent, en général, envoyer des paquets avec des adresses de source IP et contenu arbitraires, mais ces paquets pourraient être bloqués si un filtrage d'entrée [RFC2827] est appliqué. Donc, il est important de regarder l'impact du multi-rattachements sur la sécurité en présence et en l'absence de filtrage d'entrée.

1.2 Authentification, autorisation, et possession de l'identifiant

Le domaine de problème global peut être décrit en utilisant différentes terminologies.

Une façon de le décrire est qu'il est nécessaire d'abord d'authentifier l'homologue et ensuite de vérifier que l'homologue est autorisé à contrôler les localisateurs utilisés pour un identifiant particulier. Bien que ce soit correct, cela pourrait mettre trop l'accent sur l'aspect d'autorisation. Dans ce cas, l'autorisation est conceptuellement très simple ; chaque hôte (chaque identifiant) est autorisé à contrôler quels localisateurs sont utilisés pour lui-même.

Donc, il y a une façon différente de décrire la même chose. Si l'homologue peut prouver d'une manière ou d'une autre qu'il est le possesseur de l'identifiant, et si la communication est liée à l'identifiant (et non le localisateur) alors l'homologue est autorisé à contrôler les localisateurs qui sont utilisés avec l'identifiant. Cette façon de décrire le problème est utilisée dans [OWNER].

Les deux façons de regarder le problème, donc les deux ensembles de terminologie, sont utiles quand on essaye de comprendre l'espace de problème et les menaces.

2. Terminologie

Liaison : facilité de communication ou support sur lequel les nœuds peuvent communiquer à la couche de liaison, c'est-à-dire, la couche immédiatement en -dessous de IPv6. Des exemples sont les Ethernet (simples ou pontés) les liaisons PPP, X.25, le relais de trame, ou les réseaux ATM, et les "tunnels" de couche Internet (ou au dessus) comme les tunnels sur IPv4 ou IPv6 lui-même.

Interface : rattachement d'un nœud à une liaison.

Adresse : nom de couche IP qui a à la fois une signification topologique (c'est-à-dire, un localisateur) et identifie une interface. Il peut y avoir plusieurs adresses par interface. Normalement une adresse identifie de façon univoque une interface, mais il y a des exceptions : la même adresse d'envoi individuel peut être allouée à plusieurs interfaces sur le même nœud, et une adresse d'envoi à la cantonade peut être allouée à différentes interfaces sur différents nœuds.

Localisateur : nom topologique de couche IP pour une interface ou ensemble d'interfaces. Il peut y avoir plusieurs localisateurs par interface.

Identifiant : identifiant de couche IP pour un point d'extrémité de couche IP (nom de pile dans [NSRG]) qui est quelque chose qui pourrait être couramment appelé un "hôte". Le nom du point d'extrémité de transport est une fonction du protocole de transport et va normalement inclure l'identifiant IP plus un numéro d'accès. Il pourrait y avoir l'utilisation de plusieurs identifiants par pile/par hôte. Un identifiant continue de fonctionner sans considération de l'état de toute interface.

Champ d'adresse : les champs d'adresse de source et destination dans l'en-tête IPv6. Comme IPv6 est actuellement spécifié, ces champs portent des "adresses". Si les identifiants et les localisateurs sont séparés, ces champs vont contenir des

localisateurs.

FQDN *(Fully Qualified Domain Name)* : nom de domaine pleinement qualifié [RFC1983]

3. Hypothèses et attaques d'aujourd'hui

Les deux aspects de sécurité intéressants pour les solutions de multi-rattachements sont (1) l'hypothèse faite par les protocoles de couche de transport et d'application sur les identifiants qu'ils voient , et (2) les capacités existantes d'effectuer diverses attaques relatives à la relation entre identité et localisation.

3.1 Hypothèses d'application

Dans l'Internet d'aujourd'hui, la partie initiatrice des applications commence par un FQDN, qu'on cherche dans le DNS, ou elle a déjà une adresse IP par ailleurs. Pour que le FQDN effectue la recherche d'adresse IP, l'application fait effectivement confiance au DNS. Une fois qu'elle a l'adresse IP, l'application fait confiance au système d'acheminement qui livre les paquets à cette adresse. Les applications qui utilisent des mécanismes de sécurité, comme IPSEC ou TLS, ont la capacité de lier une adresse ou FQDN à du matériel de chiffrement cryptographique. Compromettre le DNS et/ou le système d'acheminement peut résulter en l'abandon de paquets ou en leur livraison à un attaquant dans ce cas, mais comme l'attaquant ne possède pas le matériel de chiffrement, l'application ne va pas faire confiance à l'attaquant, et l'attaquant ne peut pas déchiffrer ce qu'il reçoit.

À l'extrémité qui répond (non initiatrice) de la communication d'aujourd'hui, on trouve que les configurations de sécurité utilisées pas les différentes applications rentrent approximativement dans cinq classes, où une seule application pourrait utiliser différentes classes de configurations pour différents types de communication.

La première classe est l'ensemble des serveurs de contenu public. Ces systèmes fournissent des données à tous les systèmes et ne sont pas particulièrement concernés par la confidentialité, car ils rendent leur contenu disponible à tous. Cependant, ils sont intéressés à l'intégrité des données et aux attaques de déni de service. Avoir quelqu'un qui manipule les résultats d'un moteur de recherche, par exemple, ou empêche certains systèmes d'accéder à un moteur de recherche serait un sérieux problème de sécurité.

La seconde classe de configurations de sécurité utilise les adresses de source IP existantes provenant de l'extérieur de leur site local immédiat comme moyen d'authentification sans aucune forme de vérification. Aujourd'hui, avec la falsification d'adresse de source IP et les numéros de séquence TCP devinés comme attaques rampantes [RFC1948], de telles applications s'ouvrent effectivement elles mêmes à la connexité publique et s'appuient sur d'autres systèmes, comme les pare-feu, pour leur sécurité globale. On ne considère pas cette classe de configurations dans le présent document parce quelle est dans tous les cas pleinement ouverte à toutes les formes de falsification à la couche réseau.

La troisième classe de configurations de sécurité reçoit les adresses de source IP existantes, mais tente une vérification utilisant le DNS, utilisant effectivement le FQDN pour le contrôle d'accès. (Cela est normalement fait par une recherche inverse à partir de l'adresse IP, suivie par une recherche vers l'avant et la vérification que l'adresse IP correspond à une des adresses retournées de la recherche vers l'avant.) Ces applications sont déjà l'objet d'un certain nombre d'attaques utilisant des techniques comme la falsification d'adresse de source et le numéro de séquence TCP deviné car un attaquant, sachant que c'est le cas, peut simplement créer une attaque de DoS en utilisant une adresse de source falsifiée qui a des enregistrements authentiques du DNS. En général cette classe de configurations de sécurité est fortement déconseillée, mais il est probablement important qu'une solution de multi-rattachements n'introduise pas de nouvelles façons plus faciles d'effectuer de telles attaques. Cependant, on note que certains pensent qu'on devrait traiter cette classe de la même façon que la seconde classe de configurations de sécurité.

La quatrième classe de configurations de sécurité utilise des techniques de sécurité cryptographiques pour fournir à la fois une forte identité pour l'homologue et l'intégrité des données avec ou sans confidentialité. De tels systèmes sont quand même potentiellement vulnérables aux attaques de déni de service qui pourraient être introduites par un solution de multi-rattachements.

Finalement, la cinquième classe de configurations de sécurité utilise des techniques de sécurité cryptographiques, mais sans identité forte (comme IPsec opportuniste). Donc, l'intégrité des données avec ou sans confidentialité est fournie quand la communication est avec un principal inconnu/non authentifié. Tout comme la première catégorie ci-dessus, de telles applications ne peuvent pas effectuer de contrôle d'accès sur la base des informations de la couche réseau parce qu'elles ne

connaissent pas l'identité de l'homologue. Cependant, elles pourraient effectuer le contrôle d'accès en utilisant des notions d'identité de niveau supérieur. La disponibilité de IPsec (et solutions similaires) avec les liens de canal permet aux protocoles (qui, par eux-mêmes, sont vulnérables aux attaques par interposition (MITM, *man-in-the-middle*)) de fonctionner avec un fort niveau de confidentialité dans la sécurité de l'identification de l'homologue. Un exemple typique est le protocole de placement direct de données à distance (RDDP, *Remote Direct Data Placement Protocol*) qui, quand il est utilisé avec IPsec opportuniste, fonctionne bien si des liens de canal sont disponibles. Les liens de canal établissent une liaison entre l'identification de couche IP et l'identification de protocole d'application.

Une variante de la cinquième classe est celle qui utilise un "acte de foi" durant une communication initiale. Elle ne fournit pas une forte identité sauf lorsque une communication ultérieure est liée à la communication initiale, fournissant une forte assurance que l'homologue est le même que durant la communication initiale.

La cinquième classe est importante et ses propriétés de sécurité doivent être préservées par une solution multi-rattachements.

L'exigence pour une solution multi-rattachements est que la sécurité ne soit pas pire qu'elle n'est aujourd'hui dans toutes les situations. Donc, les mécanismes qui fournissent la confidentialité, l'intégrité, ou l'authentification aujourd'hui devraient continuer de fournir ces propriétés dans un environnement de multi-rattachements.

3.2 Attaques de redirection d'aujourd'hui

Ce paragraphe énumère les attaques de redirection qui sont possibles dans l'Internet d'aujourd'hui.

Si l'acheminement peut être compromis, les paquets pour toute destination peuvent être redirigés sur toute localisation. Cela peut être fait en injectant un long préfixe dans l'acheminement global, causant ainsi la livraison par l'algorithme de plus longue correspondance des paquets à l'attaquant.

De même, si le DNS peut être compromis, et si un changement peut être fait sur un enregistrement de ressource annoncé pour qu'il annonce une adresse IP différente pour un nom d'hôte, reprenant effectivement ce nom d'hôte. Des informations plus détaillées sur les menaces relatives au DNS sont dans la [RFC3833].

Tout système le long du chemin de l'hôte de source à l'hôte de destination peut être compromis et utilisé pour rediriger le trafic. Des systèmes peuvent être ajoutés au meilleur chemin pour accomplir cela. De plus, même les systèmes qui sont sur des liaisons multi-accès qui n'assurent pas la sécurité peuvent aussi être utilisés pour rediriger le trafic hors du chemin normal. Par exemple, la falsification d'ARP et ND peut être utilisée pour attirer tout le trafic pour le prochain bond légitime à travers un Ethernet. Et comme la vaste majorité des applications s'appuie sur les recherches dans le DNS, si DNSSEC n'est pas déployé, les attaquants qui sont sur le chemin entre l'hôte et les serveurs DNS peuvent aussi causer la redirection en modifiant les réponses des serveurs DNS.

En général, les attaques ci-dessus ne fonctionnent que quand l'attaquant est sur le chemin au moment où il effectue l'attaque. Cependant, dans certains cas, il est possible à un attaquant de créer une attaque de DoS qui reste au moins un certain temps après que l'attaquant a quitté le chemin. Un exemple de cela est un attaquant qui utilise la falsification d'ARP ou ND pendant qu'il est sur le chemin pour s'insérer lui-même, ou envoyer des paquets à un trou noir (une adresse de couche 2 inexistante). Après le départ de l'attaquant, les entrées d'ARP/ND vont rester dans les antémémoires des nœuds du voisinage pendant un certain temps (de l'ordre d'une minute dans le cas de ARP). Il va en résulter que des paquets continuent d'aller dans le trou noir jusqu'à ce que l'entrée d'ARP soit purgée.

Finalement, les hôtes eux-mêmes qui terminent la connexion peuvent aussi être compromis et peuvent effectuer des fonctions qui n'étaient pas prévues par l'utilisateur d'extrémité.

Toutes les attaques de protocole ci-dessus font l'ojet d'un travail en cours pour les sécuriser (DNSSEC, sécurité pour BGP, ND sûr) et ne sont pas examinées plus avant dans le présent document. Le but d'une solution de multi-rattachements n'est pas de résoudre ces attaques, c'est plutôt d'éviter d'ajouter à cette liste d'attaques.

3.3 Attaques d'injection de paquet d'aujourd'hui

Dans l'Internet d'aujourd'hui, les protocoles de couche de transport, comme TCP et SCTP, qui utilisent IP, se servent des adresses IP comme identifiants pour la communication. En l'absence de filtrage d'entrée [RFC2827], la couche IP perrmet à l'envoyeur d'utiliser une adresse de source arbitraire, donc les protocoles de transport et/ou applications doivent avoir une

protection contre les envoyeurs malveillants qui injectent des paquets bogués dans le flux de paquets entre deux homologues communicants. Si cette protection peut être circonvenue, il est alors possible à un attaquant de causer des dommages sans avoir nécessairement besoin de rediriger les paquets de retour.

Il y a divers niveaux de protection dans les différent protocoles de transport. Par exemple, en général les paquets TCP doivent contenir un numéro de séquence qui tombe dans la fenêtre du receveur pour être acceptés. Si les numéros de séquence TCP initiaux sont aléatoires, il est alors très difficile à un attaquant hors du chemin de deviner un numéro de séquence assez proche pour qu'il entre dans la fenêtre, et par suite d'être capable d'injecter un paquet dans une connexion existante. Cette difficulté va dépendre de la taille de le fenêtre disponible, de si les numéros d'accès sont aussi prévisibles, et de la durée de vie de la connexion. Noter qu'il y a un travail en cours pour renforcer la protection de TCP contre cette grande classe d'attaques [TCPSECURE]. SCTP fournit un mécanisme plus fort avec l'étiquette de vérification ; un attaquant hors du chemin va devoir deviner des nombres aléatoires de 32 bits. Bien sûr, IPsec fournit des mécanismes cryptographiquement forts qui empêchent des attaquants, sur ou hors du chemin, d'injecter des paquets une fois que les associations de sécurité ont été établies.

Quand le filtrage d'entrée est déployé entre l'attaquant potentiel et le chemin entre les homologues communicants, il peut empêcher l'attaquant d'utiliser l'adresse IP de l'homologue comme source. Dans ce cas, l'injection de paquet va échouer dans l'Internet d'aujourd'hui.

On ne s'attend pas à ce qu'une solution de multi-rattachements améliore le degré existant de prévention contre l' injection de paquets. Cependant, il est nécessaire de regarder attentivement si une solution de multi-rattachements rend plus facile aux attaquants d'injecter des paquets parce que le désir d'avoir l'homologue présent sur de multiples localisateurs, et peut-être sur un ensemble dynamique de localisateurs, peut potentiellement résulter en des solutions qui, même en présence de filtrage d'entrée, rendent plus facile l'injection de paquets.

3.4 Attaques d'inondation d'aujourd'hui

Dans l'Internet d'aujourd'hui, il y a plusieurs façons pour un attaquant d'utiliser un mécanisme de redirection pour lancer des attaques de DoS qui ne peuvent pas être facilement retracées jusqu'à l'attaquant. Un exemple en est l'utilisation de protocoles qui causent une réflexion avec ou sans amplification [PAXSON01].

La réflexion sans amplification peut être réalisée par un attaquant qui envoie in paquet TCP SYN à un serveur bien connu avec une adressse de source falsifiée ; le paquet ACK de TCP SYN résultant va être envoyé à l'adresse de source falsifiée.

Les appareils sur le chemin entre deux entités communicantes peuvent aussi lancer des attaques de DoS. Bien que de telles attaques pourraient ne pas être intéressantes aujourd'hui, il est nécessaire de mieux les comprendre afin de déterminer si une solution multi-rattachements pourrait permettre de nouveaux types d'attaques de DoS.

Par exemple, aujourd'hui, si A communique avec B, alors A peut essayer de surcharger le chemin de B à A. Si TCP est utilisé, A pourrait faire cela en envoyant des paquets ACK pour des données qu'il n'a pas encore reçu (mais qu'il soupçonne B d'avoir déjà envoyé) de sorte que B va envoyer à un taux qui pourrait causer un encombrement persistant sur le chemin vers A. Une telle attaque semblerait auto-destructrice car A va seulement faire souffrir son propre coin du réseau en surchargeant le chemin de l'Internet vers A.

Un cas plus intéressant est si A communique avec B et que X est sur le chemin entre A et B, alors X pourrait être capable de tromper B pour qu'il envoie des paquets vers A à un taux plus rapide que ce que A (et le chemin entre A et X) peut traiter. Par exemple, si TCP est utilisé, alors X peut fabriquer des paquets TCP ACK prétendant venir de A pour faire que B utilise une fenêtre d'encombrement assez grande pour causer potentiellement un encombrement persistant chez A. De plus, si X peut supprimer les paquets de A à B, il peut aussi empêcher A d'envoyer un paquet explicite "de ralentissement" à B ; c'est-à-dire, X peut désactiver tout mécanisme de contrôle de flux ou d'encombrement comme une notification explicite d'encombrement (ECN, *Explicit Congestion Notification*) [RFC3168]. Des attaques similaires peuvent probablement être lancées en utilisant des protocoles qui portent des supports de direct en faussant la notion d'accusé de réception et de rétroaction d'un tel protocole.

Un attribut de ce type d'attaque est que A va simplement penser que B est fautif car ses mécanismes de contrôle de flux et d'encombrement ne semblent pas fonctionner. Détecter que le flux de paquets de ACK est généré de X et non de A pourrait être un défi, car le taux de paquets de ACK pourrait être relativement faible. Ce type d'attaque pourrait ne pas être courant aujourd'hui parce que, en présence de filtrage d'entrée, il exige que X reste sur le chemin afin de soutenir l'attaque de DoS. Et en l'absence de filtrage d'entrée un attaquant va devoir soit être présent sur le chemin initialement et ensuite s'en aller, soit être capable d'effectuer l'établissement de communication "en aveugle", c'est-à-dire, sans voir le trafic de retour (ce qui

dans le cas de TCP, implique de deviner le numéro de séquence initial).

Le danger est que l'ajout de mécanismes de redirection multi-rattachements pourrait potentiellement supprimer la contrainte que l'attaquant reste sur le chemin. Et avec la prise en charge actuelle de non multi-rattachements, utiliser une forte sécurité de bout en bout au niveau du protocole (ou en dessous) ce traitement de "ACK" empêcherait ce type d'attaque. Mais si une solution de multi-rattachements est fournie en dessous de IPsec, ce mécanisme de prévention pourrait ne pas exister.

Donc, le défi pour les solutions de multi-rattachements est de ne pas créer des types d'attaques supplémentaires dans ce domaine, ou de rendre les types d'attaques existants significativement plus faciles.

3.5 Confidentialité de l'adresse aujourd'hui

Dans l'Internet d'aujourd'hui il y a une capacité limitée de tracer un hôte lorsque il utilise l'Internet parce que dans certains cas, comme une connexité par numérotation, l'hôte va acquérir une adresse IP différente chaque fois qu'il se connecte. Cependant, avec l'utilisation croissante de la connexité large bande, comme le DSL ou le câble, il devient de plus en plus probable que l'hôte va conserver la même adresse IPv4 au fil du temps. Si un hôte se déplace dans l'Internet d'aujourd'hui, par exemple, en visitant des sites WiFi, il va être configuré avec une adresse IPv4 différente sur chaque site.

On observe aussi qu'une pratique courante dans IPv4 aujourd'hui est d'utiliser une forme de traduction d'adresse, que le site soit multi-rattaché ou non. Cela cache effectivement l'identité de l'hôte spécifique au sein d'un site ; seul le site peut être identifié sur la base de l'adresse IP.

Dans les cas où il est souhaitable de conserver la connexité lorsque l'hôte se déplace, en utilisant une technologie de couche 2 ou IPv4 mobile, l'adresse IPv4 va rester constante durant le mouvement (autrement les connexions seraient rompues). Donc, il y a une sorte de choix aujourd'hui entre une connexité sans coupure durant le mouvement et une confidentialité accrue de l'adresse.

Aujourd'hui, quand un site est multi-rattaché à plusieurs FAI, l'établissement courant est qu'un seul préfixe d'adresse IP est utilisé avec tous les FAI. Par suite, il est possible de tracer qu'il est le même hôte qui est en communication via tous les FAI.

Cependant, quand un hôte (et non un site) est multi-rattaché à plusieurs FAI (par exemple, par une connexion du service général de radiocommunication en mode paquet (GPRS, *General Packet Radio Service*) et un point d'accès public sans fil) l'hôte reçoit différentes adresses IP sur chaque interface. Bien que le travail sur le multi-rattachements se concentre sur le multi-rattachements de site, si la solution devait aussi être applicable au multi-rattachements d'hôte, l'impact sur la confidentialité devrait être aussi considéré pour ce cas.

L'auto-configuration d'adresse IPv6 sans état facilite la gestion des adresses IP, mais soulève des questions car l'adresse Ethernet est codée dans les 64 bits de moindre poids de l'adresse IPv6. Cela pourrait potentiellement être utilisé pour tracer un hôte lorsque il se déplace dans le réseau, en utilisant différents FAI, etc. IPv6 spécifie des adresses temporaires [RFC3041],qui permettent aux applications de contrôler si elles ont besoin d'adresses IPv6 de longue durée ou si elles désirent une confidentialité améliorée avec l'usage d'adresses temporaires.

Étant donné qu'il n'y a pas aujourd'hui de confidentialité d'adresse dans les établissements de site multi-rattachements, le problème principal pour le critère de "pas de dommage" est de s'assurer que les hôtes qui se déplacent ont toujours la même capacité que dans l'Internet d'aujourd'hui de choisir entre connexité sans coupure et confidentialité d'adresse améliorée, et aussi que l'introduction de la prise en charge du multi-rattachements devrait quand même fournir la même capacité qu'on a dans IPv6 avec les adresses temporaires.

Quand on examine les menaces pour la confidentialité, il est raisonnable de distinguer les attaques faites par de entités sur le chemin qui observent les paquets qui s'écoulent, et les attaques par l'homologue communicant. Il est probablement faisable d'empêcher les entités sur le chemin de corréler les multiples adresses IP de l'hôte; mais le fait que l'homologue doive être informé des multiples adresses IP afin d'être capable de passer à l'utilisation d'adresses différentes quand la communication échoue, limite la capacité de l'hôte à empêcher de corréler ses multiples adresses. Cependant, l'utilisation de plusieurs pseudonymes pour un hôte devrait être capable de traiter ce cas.

4. Nouvelles attaques potentielles

Cette Section documente les attaques supplémentaires qui ont été découvertes résultant d'une architecture où les hôtes peuvent changer leur connexion topologique au réseau au milieu d'une session de transport sans interruption. Cette discussion est là encore articulée dans le contexte où les localisateurs topologiques peuvent être indépendants des identifiants d'hôte utilisés par les protocoles de couche de transport et d'application. Certaines de ces attaques peuvent n'être pas applicables si des adresses traditionnelles sont utilisées. Cette Section suppose que chaque hôte a plusieurs localisateurs et qu'il y a un mécanisme pour déterminer les localisateurs pour l'hôte correspondant. On ne suppose rien sur les propriétés de ces mécanismes. Cette liste servira plutôt à nous aider à déduire les propriétés de ces mécanismes qui vont être nécessaires pour empêcher ces attaques de redirection.

Selon l'objet de l'attaque de redirection, on sépare les attaques en plusieurs types différents.

4.1 Causer l'envoi des paquets à l'attaquant

Un attaquant pourrait vouloir recevoir le flux de paquets, par exemple pour être capable d'inspecter et/ou modifier la charge utile pour être capable d'appliquer une analyse cryptographique à la charge utile protégée cryptographiquement, en utilisant des attaques de redirection.

Noter que de telles attaques sont toujours possibles aujourd'hui si un attaquant est sur le chemin entre deux parties communicantes, et une solution de multi-rattachements ne peut pas supprimer cette menace. Donc, le gros de ces problèmes se rapporte à des attaquants hors chemin.

4.1.1 Une fois que les paquets s'écoulent

Cela peut être vu comme l'attaque de redirection "classique".

Quand A et B sont en communication, X pourrait envoyer des paquets à B et prétendre : "Hé, je suis A, j'envoie mes paquets à ma nouvelle situation." alors que cette situation est en fait celle de X.

Les solutions "standard" à cela incluent d'exiger qu'il soit vérifié que l'hôte qui demande une redirection est bien le même hôte que l'hôte initial qui a établi la communication. Cependant, la charge d'une telle vérification ne doit pas être onéreuse, ou les demandes de redirection elles-mêmes pourraient être utilisées comme attaque de DoS.

Pour empêcher ce type d'attaque, une solution va avoir besoin d'un mécanisme que B puisse utiliser pour vérifier si un localisateur appartient à A avant que B commence à utiliser ce localisateur, et être capable de faire cela quand plusieurs localisateurs sont alloués à A.

4.1.2 Attaque en temps glissant

Le terme "attaque en temps glissant" est utilisé pour décrire la capacité d'un attaquant à effectuer une attaque après qu'il n'est plus sur le chemin. Donc, l'attaquant devra avoir été sur le chemin à un moment, espionnant et/ou modifiant les paquets, et plus tard, quand l'attaquant n'est plus sur le chemin, il lance l'attaque.

Dans l'Internet actuel, il n'est pas possible d'effectuer de telles attaques pour rediriger les paquets. Mais pendant un certain temps après son départ, l'attaquant peut causer une attaque de DoS, par exemple, en laissant une entrée d'ARP boguée dans les nœuds sur le chemin, ou en falsifiant des paquets TCP Reset sur la base des numéros de séquence initiaux TCP vus quand il était sur le chemin.

Il serait raisonnable d'exiger qu'une solution de multi-rattachements limite la capacité de rediriger et/ou dénier le service au trafic à quelques minutes après que l'attaquant a quitté le chemin.

4.1.3 Redirection préméditée

C'est une variante de l'attaque ci-dessus où l'attaquant "s'installe" avant le début de la communication.

Par exemple, si l'attaquant X peut prédire que A et B vont communiquer dans un proche avenir, l'attaquant peut alors dire à B: "Hé, je suis A et je suis à cet endroit". Quand plus tard A essaye de communiquer avec B, est-ce que B va croire qu'il est

réellement A ?

Si la solution à l'attaque de redirection classique est fondée sur "prouve que tu es le même qu'initialement", alors A va échouer à prouver cela à B parce que X a initié la communication.

Selon les détails qui vont être spécifiques d'une solution proposée, ce type d'attaque pourrait causer la redirection (de sorte que les paquets destinés à A vont être envoyés à X) ou pourrait causer un déni de service (où A échouerait à communiquer avec B car il ne peut pas prouver qu'il est le même hôte que X).

Pour empêcher cette attaque, la vérification de si un localisateur appartient à l'homologue ne peut pas être simplement fondée sur le premier homologue qui prend contact.

4.1.4 Utilisation des attaques en répétition

Bien que le problème du multi-rattachements n'implique pas par lui-même de mouvement topologique, il est utile aussi de considérer l'impact du renumérotage de site en combinaison avec le multi-rattachements. Dans ce cas, l'ensemble de localisateurs pour un hôte va changer chaque fois que son site est dénuméroté, et, à un certain moment après un événement de renumérotage, le vieux préfixe de localisateur pourrait être réalloué à un autre site.

Cela donne potentiellement à un attaquant la capacité de répéter le mécanisme de protocole qui a été utilisé pour informer un hôte des localisateurs d'un homologue de sorte que l'hôte va incorrectement être conduit à croire que l'ancien (ensemble de) localisateur devrait être utilisé même longtemps après un événement de renumérotage. Ceci est similaire au risque de répétition des mises à jour de lien de la [RFC3775], mais la constante de temps est assez différente ; IPv6 mobile pourrait voir des mouvements chaque seconde tandis que le renumérotage de site, suivi par la ré allocation du préfixe du localisateur du site, pourrait être une affaire de semaines ou de mois.

Pour empêcher de telles attaques en répétition, le protocole utilisé pour vérifier quels localisateurs peuvent être utilisés avec un identifiant particulier a besoin d'un mécanisme de protection contre la répétition.

Aussi, dans cet espace on doit se préoccuper de potentielles interactions entre une telle protection contre la répétition et l'acte administratif de réallocation d'un localisateur. Si la relation entre l'identifiant et le localisateur est distribuée dans le réseau, on va devoir s'assurer que les vieilles informations ont été complètement purgées du réseau avant toute réallocation. Noter que cela n'exige pas un mécanisme explicite. Cela peut plutôt être mis en œuvre par la politique de réutilisation de localisateur et des temporisations appropriées des informations de localisateur.

4.2 Causer l'envoi des paquets à un trou noir

C'est aussi une variante de l'attaque de redirection classique. La différence est que la nouvelle localisation est un localisateur qui est non existant ou injoignable. Donc, l'effet est que l'envoi de paquets au nouveau localisateur cause l'élimination des paquets ailleurs dans le réseau.

On s'attendrait à ce que des solutions qui empêchent les précédentes attaques de redirection empêchent cette attaque par un effet collatéral, mais il est raisonnable d'inclure ici cette attaque pour être complet. Les mécanismes qui ont empêché une attaque de redirection pour l'attaquant devraient aussi empêcher la redirection sur un trou noir.

4.3 Attaques de déni de service par un tiers

Un attaquant peut utiliser la capacité d'effectuer une redirection pour causer la surcharge d'un tiers sans rapport. Par exemple, si A et B communiquent, alors l'attaquant X pourrait être capable de convaincre A d'envoyer les paquets destinés à B à un nœud C tiers. Bien que cela puisse sembler à première vue sans dommage, comme X pourrait juste inonder directement C avec des paquets, il y a quelques aspects de ces attaques qui causent des problèmes.

Le premier est que l'attaquant pourrait être capable de cacher complètement son identité et sa localisation. Il pourrait suffire que X envoie et reçoive quelques paquets pour A pour effectuer la redirection, et A ne pourrait pas conserver d'état sur qui a demandé la redirection sur la localisation de C. Même si A avait conservé un tel état, cet état ne serait probablement pas facilement disponible pour C, donc C ne peut pas déterminer qui était l'attaquant une fois que C est devenu la victime d'une attaque de déni de service.

Le second souci est que, avec une attaque de Dos directe de X sur C, l'attaquant est limité par la bande passante de son

propre chemin vers C. Si l'attaquant peut amener un autre hôte, comme A, à rediriger son trafic sur C, alors la bande passante est limitée par le chemin de A à C. Si A est un service Internet à forte capacité et si X a une connexité lente (par exemple, par numérotation) cette différence pourrait être substantielle. Donc, en effet, cela pourrait être similaire aux réflecteurs d'amplification de paquets dans [PAXSON01].

Le troisième souci final est que si un attaquant a seulement besoin de quelques paquets pour convaincre un hôte d'inonder un tiers, il serait alors difficile à l'attaquant de convaincre beaucoup d'hôtes d'inonder le même tiers. Donc, cela pourrait être utilisé pour des attaques distribuées de déni de service.

Une attaque de DoS de tiers pourrait être contre les ressources d'un hôte particulier (c'est-à-dire, C dans l'exemple ci-dessus) ou elle pourrait être contre l'infrastructure du réseau sur un préfixe d'adresse IP particulier, en surchargeant les routeurs ou les liaisons même si il n'y a pas d'hôte à l'adresse ciblée.

Dans l'Internet d'aujourd'hui, la capacité d'effectuer ce type d'attaque est assez limitée. Pour que l'attaquant initie la communication, il va dans la plupart des cas devoir être capable de recevoir des paquets de l'homologue (avec une exception potentielle pour les techniques qui combinent cela avec les techniques consistant à deviner le numéro de séquence de TCP). De plus, dans la mesure où des parties de l'Internet utilisent le filtrage d'entrée [RFC2827], même si la communication pourrait être initiée, il ne serait pas possible de la soutenir par l'envoi de paquets ACK avec des adresses falsifiées d'un attaquant hors du chemin.

Si ce type d'attaque ne peut pas être empêché, il peut y avoir des techniques d'atténuation à employer. Par exemple, dans le cas de TCP une défense partielle peut être construite par le déclenchement du démarrage lent de TCP quand le localisateur de destination change. (On pourrait objecter que, indépendamment de la sécurité, cela serait l'action correcte pour le contrôle d'encombrement car TCP pourrait ne pas avoir d'informations relatives à l'encombrement sur le nouveau chemin impliqué par le nouveau localisateur.) On peut supposer que la même approche peut être appliquée aux autres protocoles de transport qui effectuent des formes différentes de contrôle d'encombrement (favorables à TCP) même si certaines d'entre elles pourraient ne pas s'adapter aussi rapidement que TCP. Mais comme tous les protocoles de contrôle d'encombrement ont probablement besoin d'avoir une réaction au changement de chemin impliqué par un changement de localisateur, il paraît raisonnable de penser aux attaque de DoS de tiers quand on conçoit comment les protocoles de transport spécifiques devraient réagir à un changement de localisateur. Cependant, cela serait seulement une solution partielle car cela prendrait probablement plusieurs paquets et aller-retours avant que le protocole de transport cesse de transmettre ; donc, un attaquant pourrait encore utiliser cela comme un réflecteur avec l'amplification de paquet. Donc, le mécanisme de multi-rattachements a probablement besoin d'une forme de défense contre les attaques de DoS de tiers, en plus de l'aide qu'il peut obtenir des protocoles de transport.

4.3.1 DoS de tiers de base

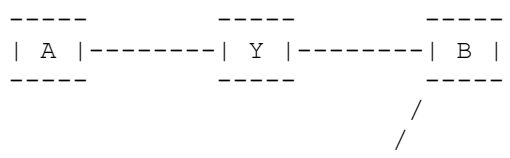
Supposons que X soit sur une liaison lente n'importe où dans l'Internet. B est sur une liaison rapide (gigabits, par exemple, un serveur de supports) et A est la victime.

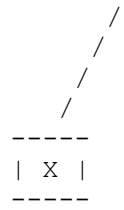
X pourrait inonder A directement mais est limité par sa faible bande passante. Si X peut établir une communication avec B, demander à B de lui envoyer un flux de supports à grande vitesse, alors X peut probablement falsifier le "retour/accusé de réception" nécessaire pour que B envoie des paquets à tout vitesse. Jusque là, cela atteint seulement X et le chemin entre X et l'Internet. Mais si X pourrait aussi dire à B "Je suis Ie localisateur de A", alors X aura effectivement utilisé cette capacité de redirection dans le multi-rattachements pour amplifier sa capacité de DoS, ce qui serait une source de problèmes.

On pourrait envisager des techniques assez simples pour empêcher de telles attaques. Par exemple, avant d'envoyer à un nouveau localisateur homologue, effectuer un échange en clair avec le nouveau localisateur prétendu de la forme "Êtes vous X ?" résultant en "Oui, je suis X.". Cela suffirait pour les plus simples attaques. Cependant, comme on va le voir ci-dessous, des attaques plus sophistiquées sont possibles.

4.3.2 DoS de ties avec aide en chemin

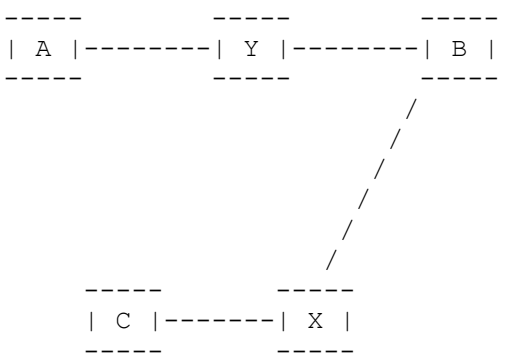
Le scénario est le même que ci-dessus, mais, en plus, l'attaquant X a un ami Y sur le chemin entre A et B :





Avec la solution simple suggérée au paragraphe précédent, tout ce dont Y a besoin est de fabriquer une réponse au paquet "Est tu X ?", et après ce moment Y pourrait n'être pas nécessaire ; X pourrait potentiellement soutenir le flux de données vers A en générant les paquets de ACK. Donc, il serait encore plus difficile de détecter l'existence de Y.

De plus, si X n'est pas le système d'extrémité réel mais un attaquant entre un nœud C et B, alors X peut prétendre être C, et aucun doigt ne peut être pointé non plus sur X :



Donc, avec deux attaquants sur des chemins différents, il pourrait ne pas y avoir de trace de qui a fait la redirection sur le tiers une fois que la redirection a eu lieu.

Un cas spécifique de ceci est quand X = Y, et X est situé sur le même LAN que B.

Une façon potentielle de rendre de telles attaques plus difficiles serait d'utiliser le dernier localisateur de source reçu (et vérifié) comme localisateur de destination. De cette façon, quand X envoie les paquets de ACK (qu'il prétende être X ou C) le résultat serait que le flux de paquet provenant de B va revenir sur X/C, ce qui résulterait en une attaque similaire à ce qui peut être effectué dans l'Internet d'aujourd'hui.

Une autre façon de rendre ces attaques plus difficiles serait d'effectuer des vérifications périodiques que l'homologue est disponible au localisateur, au lieu de juste quand le nouveau localisateur est reçu.

Une troisième façon dont une solution de multi-rattachements pourrait traiter cela est de s'assurer que B va seulement accepter les localisateurs qui peuvent être authentifiés comme synonymes du correspondant original. Il doit être possible de s'assurer en toute sécurité que ces localisateurs forment une classe d'équivalence. Donc dans le premier exemple, non seulement X doit affirmer qu'il est A, mais A doit affirmer qu'il est X.

4.4 Acceptation de paquets provenant de localisateurs inconnus

L'espace de solutions de multi-rattachements n'affecte pas seulement la destination des paquets ; il soulève aussi la question de quelles sources les paquets devraient être acceptés. Il est possible de construire une solution de multi-rattachements qui permette au trafic d'être reconnu comme venant du même homologue même si il y a un localisateur précédemment inconnu présent dans le champ d'adresse de source. La question est si on veut permettre aux paquets provenant de sources non vérifiée d'être passés aux protocoles de couche de transport et d'application.

Dans l'Internet actuel, un attaquant ne peut pas injecter des paquets avec des adresses de source arbitraires dans une session si le filtrage d'entrée est présent, permettant ainsi aux paquets qui ont des sources non vérifiées dans une solution multi-rattachements d'échouer à notre essai tournesol "pas pire que ce qu'on a actuellement". Cependant, étant donné que le déploiement du filtrage d'entrée est loin d'être universel et que le filtrage d'entrée ne va normalement pas empêcher de falsifier des adresses dans le même sous-réseau, exiger de rejeter les paquets provenant de localisateurs non vérifiés pourrait être trop contraignant.

Un exemple de l'état actuel est la capacité d'injecter des paquets RST dans les connexions TCP existantes. Quand il n'y a pas de filtrage d'entrée dans le réseau, c'est quelque chose que les points d'extrémité TCP doivent régler eux-mêmes. Cependant, déployer le filtrage d'entrée aide dans l'Internet d'aujourd'hui car un attaquant est limité quant à l'ensemble d'adresses de source qu'il peut utiliser.

Un facteur à prendre en compte pour déterminer le "niveau d'exigence" pour cela est que quand IPsec est utilisé par dessus la solution de multi-rattachements, IPsec va rejeter ces paquets falsifiés. (Noter que ceci est différent du cas de l'attaque de redirection où même avec IPsec un attaquant pourrait potentiellement causer une attaque de DoS.)

Il pourrait aussi y avoir un moyen terme où des attaquants arbitraires sont empêchés d'injecter des paquets en utilisant le type d'approche de l'étiquette de vérification SCTP [RFC2960]. (C'est une étiquette en clair qui est envoyée à l'homologue, que l'homologue est supposé inclure dans chaque paquet suivant.) Une telle approche n'empêche pas l'injection de paquets par des attaquants dans le chemin (car ils peuvent observer l'étiquette de vérification) mais le filtrage d'entrée ne le fait pas non plus.

4.5 Nouvelles considérations de confidentialité

Bien que l'introduction d'identifiants puisse être utile en fournissant des moyens pour identifier les hôtes à travers des événements quand leurs adresses IP changent, il y a un risque que ces mécanismes puissent être utilisés pour suivre l'identité de l'hôte sur de longues périodes, si ils utilisent le même (ensemble de) FAI ou se déplacent entre différents points de rattachement au réseau. Les concepteurs de solutions de multi-rattachements doivent être conscients de ce problème.

Introduire la capacité de multi-rattachements implique par nature que les homologues communicants doivent connaître plusieurs localisateurs pour chaque autre afin d'être résilients aux défaillances de certains chemins/localisateurs. De plus, si le protocole de signalisation de multi-rattachements n'assure pas la confidentialité, il serait possible à des tiers sur le chemin de découvrir beaucoup ou tous les localisateurs alloués à un hôte, ce qui augmenterait l'exposition de la confidentialité comparée à celle d'un hôte multi-rattaché d'aujourd'hui.

Par exemple, une solution pourrait traiter cela en permettant que chaque hôte ait plusieurs identifiants en même temps et peut-être même de changer l'ensemble d'identifiants qui sont utilisés au fil du temps. Cette approche pourrait être analogue à ce qui est fait pour les adresses IPv6 dans la [RFC3041].

5. Granularité de redirection

Différentes solutions de multi-rattachements pourraient approcher le problème à différentes couches de la pile de protocoles. Par exemple, il y a eu des propositions pour une couche d'ajustement à l'intérieur de IP, ainsi que des approches à la couche transport. La première aurait la capacité de rediriger une adresse IP tandis que la seconde pourrait être contrainte de seulement rediriger une seule connexion de transport. Cette différence pourrait être importante quand on en vient à comprendre l'impact sur la sécurité.

Par exemple, des attaques préméditées pourraient avoir un impact assez différent dans les deux cas. Dans un solution multi-rattachements fondée sur IP une redirection préméditée réussie pourrait être due à ce que l'attaquant se connecte à un serveur et prétende être 'A', ce qui aurait pour résultat que le serveur conserverait de l'état sur 'A', qu'il aurait reçu de l'attaquant. Plus tard, quand le 'A' réel essaye de se connecter au serveur, l'existence de cet état pourrait signifier que 'A' échoue à communiquer, ou que ses paquets sont envoyés à l'attaquant. Mais si le même scénario est appliqué à une approche de couche transport, alors l'état créé du fait de l'attaquant va peut-être être limité à la connexion de transport existante. Donc, alors que cela pourrait empêcher le 'A' réel de se connecter au serveur quand l'attaquant est connecté (si il se trouve utiliser le même numéro d'accès de transport) cela ne va très probablement pas affecter la capacité de 'A' de se connecter après que attaquant s'est déconnecté.

Un aspect particulier de la question de la granularité est la question de la direction : l'état créé va-t il être utilisé pour la communication dans la direction inverse de celle de sa création ? Par exemple, si l'attaquant 'X' suspecte que 'A' va se connecter à 'B' dans le futur proche, X peut il se connecter à A et prétendre être B, et faire ensuite que ce dernier fasse connecter A à l'attaquant au lieu du B réel ?

Noter que les approches de couche transport sont limitées à l'ensemble des protocoles de "transport" que la mise en œuvre rend sensibles au multi-rattachements. Dans de nombreux cas, il va y avoir des protocoles de "transport" qui sont inconnus

de la capacité de multi-rattachements du système, comme les applications construites par dessus UDP. Pour comprendre l'impact de la question de la granularité sur la sécurité, on aurait aussi besoin de comprendre comment de telles applications/protocoles vont être traités.

Une propriété de la granularité du transport est que la quantité de travail effectué par un hôte légitime est proportionnelle au nombre de connexions de transport qu'il crée; qui utilisent la prise en charge du multi-rattachements, car chacune de ces connexions va exiger une signalisation de multi-rattachements. Et la même chose est vraie pour l'attaquant. Cela signifie qu'un attaquant pourrait probablement faire une attaque préméditée pour toutes les connexions TCP à l'accès 80 de A à B, en établissant 65 536 (pour tous les numéros d'accès de source TCP) connexions au serveur B et en faisant croire à B que ces connexions devraient être dirigées sur l'attaquant et en gardant ces connexions TCP ouvertes. Toute tentative de rendre plus efficace la communication légitime (par exemple, en étant capable de signaler à un moment plusieurs connexions de transport) fournirait autant d'avantage relatif à un attaquant qu'aux hôtes légitimes.

La question n'est pas seulement sur l'espace (granularité) mais aussi sur le composant durée de vie dans les résultats d'une demande de multi-rattachements. Dans une approche de couche transport, l'état de multi-rattachements serait probablement détruit quand l'état de transport est supprimé au titre de la fermeture de la connexion. Mais une approche de couche IP devrait s'appuyer sur des mécanismes de temporisation ou de collecte des détritus, peut être combinés avec une nouvelle signalisation explicite, pour supprimer l'état de multi-rattachements. Le couplage entre l'état de la connexion et l'état de multi-rattachements dans l'approche de couche transport pourrait la rendre plus coûteuse pour l'attaquant, car il doit garder les connexions ouvertes.

En résumé, il y a des problèmes qui ne sont pas encore bien compris sur la granularité et la réutilisation de l'état de multi-rattachements.

6. Implications de mouvement ?

Dans le cas où rien ne bouge, nous avons une compréhension raisonnable des exigences de sécurité. Quelque chose qui est sur le chemin peut être un interposé (MITM) dans l'Internet d'aujourd'hui, et une solution de multi-rattachements n'a pas besoin de rendre plus sûr cet aspect.

Mais il est plus difficile de comprendre les exigences quand les hôtes sont en mouvement. Par exemple, un hôte pourrait être sur le chemin pour un court moment en infectant un point d'accès public 802.11. Serait on ou non concerné si une telle infection (que beaucoup appellent une attaque "en temps glissant") résultait en ce que l'hôte temporairement sur le chemin soit capable d'agir comme interposé pour les futures communications ? Selon la solution, cela serait possible si l'attaquant cause la création d'un état de multi-rattachements chez divers hôtes homologues tandis que l'attaquant était sur le chemin, et que l'état est resté pendant un certain temps chez les homologues.

La réponse à cette question ne paraît pas évidente même en l'absence de toute nouvelle prise en charge du multi-rattachements. On n'a pas beaucoup d'expérience d'hôtes en mouvement qui soient capables d'attaquer des choses pendant qu'ils bougent. Dans IPv6 mobile [RFC3775] une approche prudente a été retenue qui limite l'effet de telles attaques induites à la durée de vie maximum du lien, qui est réglée à quelques minutes.

Avec la prise en charge du multi-rattachements la question devient un peu plus compliquée parce que on veut explicitement permettre à un hôte d'être présent sur plusieurs localisateurs en même temps. Donc, il pourrait y avoir besoin de distinguer entre l'hôte qui se meut entre différents localisateurs, et l'hôte qui envoie des paquets avec des localisateurs de source différents parce que il est présent sur plusieurs localisateurs sans aucun mouvement topologique.

Noter que les solutions de multi-rattachements qui ont été discutées vont des attaques "induites" rendues impossibles (par exemple, dues à un fort lien à un identifiant séparé comme dans HIP, ou dues à l'appui de la sécurité relative du DNS pour transmettre, plus les recherches inverses dans un NOID) aux systèmes qui sont au premier arrivé, premier servi (WIMP étant un exemple avec un espace d'identifiant séparé, une approche MAST avec un PBK qui est un exemple sans espace d'identifiant séparé) qui permet au premier hôte qui utilise un identifiant/adresse de la revendiquer sans limite de temps.

7. Autres problèmes de sécurité

Les mécanismes de protocole ajoutés au titre d'une solution de multi-rattachements ne devraient pas introduire de nouveau déni de service dans les mécanismes eux-mêmes. En particulier, il faut veiller à ne pas :

- créer d'état sur le premier paquet d'un échange, car il pourrait en résulter une attaque de consommation d'état similaire à l'attaque d'inondation de SYN TCP,
- effectuer plus de travail sur le premier paquet dans un échange (comme une vérification coûteuse).

Il y a ici un potentiel problème de la poule et de l'œuf, parce que on veut potentiellement éviter de faire du travail ou de créer de l'état jusqu'à ce que l'homologue ait été vérifié, mais la vérification va probablement avoir besoin d'un peu d'état et de travail pour être faite. Éviter tout travail ne semble pas possible, mais une bonne conception de protocole peut souvent retarder la création d'état jusqu'à ce que la vérification soit achevée.

Une approche possible que les solutions pourraient investiguer est de différer la vérification jusqu'à ce qu'il apparaisse qu'il y a deux hôtes différents (ou deux localisateurs différents pour le même hôte) qui veulent utiliser le même identifiant. Dans ce cas, on va devoir examiner si une combinaison d'usurpation d'identité et une attaque de DoS peut être utilisée pour empêcher la découverte de l'usurpation d'identité.

Une autre approche possible est de d'abord établir les communications, et ensuite d'effectuer la vérification en parallèle avec des transferts de données normaux. La redirection ne serait permise qu'après l'achèvement de la vérification, mais avant que cela arrive, les données pourrait être transférées de manière normale, non multi rattachée.

Finalement, les nouveaux mécanismes de protocole devraient être protégés contre les paquets falsifiés, au moins provenant de sources hors chemin, et les paquets répétés.

8. Considérations sur la sécurité

À la Section 3, le document a présenté des attaques de redirection existantes fondées sur le protocole. Mais il y a aussi des attaques de redirection non fondées sur le protocole. Un attaquant qui peut gagner l'accès physique au fil de cuivre ou à la fibre quelque part dans le chemin, à un routeur ou appareil de couche 2 dans le chemin, ou à un des systèmes d'extrémité peut aussi rediriger les paquets. Cela serait possible, par exemple, par une intrusion physique ou en corrompant le personnel qui a accès à l'infrastructure physique. De telles attaques sortent du domaine de cette discussion, mais il vaut la peine de s'en souvenir quand on examine le coût pour un attaquant d'exploiter les attaques fondées sur le protocole par rapport à des solutions de multi-rattachements ; rendre les attaques fondées sur le protocole beaucoup plus coûteuses à lancer que des attaques du type intrusion/corruption pourrait être exagéré.

9. Remerciements

Ce document a été à l'origine produit par une équipe de conception MULTI6 composée de (par ordre alphabétique) : Iljitsch van Beijnum, Steve Bellovin, Brian Carpenter, Mike O'Dell, Sean Doran, Dave Katz, Tony Li, Erik Nordmark, et Pekka Savola.

Beaucoup de la connaissance de ces menaces vient du travail sur IPv6 mobile [RFC3775], [RFC4225], [AURA02].

Comme le document a évolué, les participants au groupe de travail MULTI6 ont contribué au document. En particulier : Masataka Ohta a apporté les considérations de confidentialité relatives aux identifiants stables. La suggestion de discuter la granularité du transport contre celle de IP a été apportée par Marcelo Bagnulo, qui a aussi contribué au texte de l'Appendice B. De nombreuses précisions rédactionnelles viennent de Jari Arkko.

10. Références pour information

[AURA02] Aura, T. and Arkko, "MIPv6 BU Attacks and Defenses", Travail en cours, mars 2002.

[CBHI] Iljitsch van Beijnum, "Crypto Based Host Identifiers", Travail en cours, février 2004.

[HIP] Pekka Nikander, "Considerations on HIP based IPv6 multi-homing", Travail en cours, juillet 2004.

[NOID] Erik Nordmark, "Multihoming without IP Identifiers", Travail en cours, juillet 2004.

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

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

[PAXSON01] V. Paxson, "An Analysis of Using Reflectors for Distributed Denial-of-Service Attacks", Computer Communication Review 31(3), juillet 2001.

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

[RFC1948] S. Bellovin, "Se défendre contre les attaques de numéro de séquence", mai 1996. (*Obsolète, voir* RFC6528) *(Info.)*

[RFC1983] G. Malkin, "Glossaire des utilisateurs de l'Internet", FYI 18, août 1996.

[RFC2827] P. Ferguson, D. Senie, "Filtrage d'entrée de réseau : Combattre les attaques de déni de service qui utilisent l'usurpation d'adresse de source IP", mai 2000. (*MàJ par* RFC3704) (BCP0038)

[RFC2960] R. Stewart et autres, "Protocole de transmission de commandes de flux", octobre 2000. (*Obsolète, voir* RFC4960) *(P.S.)*

[RFC3041] T. Narten, R. Draves, "Extensions de confidentialité pour l'auto-configuration d'adresse sans état dans IPv6", janvier 2001. (*Obsolète, voir* RFC4941) *(P.S.)*

[RFC3168] K. Ramakrishnan et autres, "Ajout de la notification explicite d'encombrement (ECN) à IP", DOI 10.17487/RFC3168, septembre 2001. *(P.S. ; MàJ par* RFC8311)

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

[RFC3833] D. Atkins, R. Austein, "Analyse des menaces contre le système des noms de domaines (DNS)", août 2004. *(Info.)*

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

[TCPSECURE] M. Dalal (ed), "Transmission Control Protocol security considerations", Travail en cours, novembre 2004.

[WIMP] Jukka Ylitalo, "Weak Identifier Multihoming Protocol (WIMP)", Travail en cours, juin 2004.

Appendice A. Analyse de la sécurité

Quand on examine les propositions qui ont été faites pour les solutions de multi-rattachements et les menaces ci-dessus, il semble qu'il y a deux aspects distincts du traitement des menaces de redirection :
- Redirection de la communication existante,
- Redirection d'une identité avant toute communication.

Cela semble être en rapport avec le fait qu'il y a deux différentes classes d'utilisation des identifiants. Une utilisation est pour :
- o Établir initialement la communication ; chercher un FQDN pour trouver quelque chose qui est passé à une invocation d'API connect() ou sendto().
- o Comparer si une entité homologue est la même entité homologue que dans une communication précédente.
- o Utiliser l'identité de l'homologue pour une future communication ("rappels") dans la direction inverse, ou pour se référer à un tiers ("références").

L'autre utilisation des identifiants est au tittre de la capacité de rediriger une communication existante pour utiliser un localisateur différent.

La première classe d'utilisations semble être relative à quelque chose sur la propriété de l'identifiant ; prouver la "propriété" de l'identifiant devrait être suffisant pour être autorisé à contrôler quels localisateurs sont utilisés pour atteindre l'identifiant.

La seconde classe d'utilisations semble se rapporter à quelque chose de plus éphémère. Afin de rediriger la communication existante sur un autre localisateur, il semble être suffisant de prouver que l'entité est la même que celle qui a initié la communication. On peut voir cela comme prouver la propriété d'un certain contexte, où le contexte est établi autour du moment où la communication est initiée.

Empêcher la redirection non autorisée d'une communication existante peut être traité par un grand nombre d'approches qui se fondent que l'établissement d'une forme de matériel de sécurité au début de la communication, et d'utiliser plus tard l'existence de ce matériel pour qu'une extrémité prouve à l'autre qu'elle reste la même. Un exemple de cela est celui des clés construites à dessein [PBK]. On peut envisager différentes approches pour de tels schémas avec différentes complexités, performances, et sécurité résultante comme dans l'échange Diffie-Hellman anonyme, les chaînes de hachage inverse présentées dans [WIMP], ou même un échange de jeton en clair dans la communication initiale.

Cependant, les mécanismes pour empêcher l'utilisation non autorisée d'un identifiant peuvent être assez différents. Une façon d'empêcher la redirection préméditée est de simplement ne pas introduire un nouvel espace de nom d'identifiant, et de s'appuyer plutôt sur un ou des espaces de noms existants, un tiers de confiance, et une façon suffisamment sûre d'accéder au tiers, comme dans [NOID]. Cette approche s'appuie sur le tiers (le DNS dans le cas de NOID) comme fondation. En termes de création d'état de multi-rattachements, dans ce cas la redirection préméditée est aussi facile ou aussi difficile que de rediriger une adresse IP aujourd'hui. Essentiellement, cela s'appuie sur la vérification d'acheminement de retour associé à un aller-retour de communication, qui vérifie que le système d'acheminement livre les paquets à l'adresse IP en question.

Autrement, on peut utiliser les identifiants fondés sur la cryptographie comme dans [HIP] ou les adresses générées cryptographiquement comme dans [CBHI], qui tous deux s'appuient sur un chiffrement de clé publique, pour empêcher les attaques préméditées. Dans certains cas, il est aussi possible d'éviter le problème en faisant qu'une extrémité de la communication utilise des identifiants éphémères comme l'initiateur le fait dans [WIMP]. Cela évite la redirection préméditée en détectant qu'une autre entité utilise le même identifiant chez l'homologue et en passant à l'utilisation d'un autre identifiant éphémère. Bien que les identifiants éphémères pourraient être problématiques quand ils sont utilisés par les applications, par exemple à cause de rappels ou de références, on note que pour l'extrémité qui a l'identifiant éphémère, on peut contourner les attaques préméditées (en supposant que la solution a une façon robuste de prendre un nouvel identifiant quand un est utilisé/volé).

En supposant que le problème ne peut pas être contourné par l'utilisation d'identifiants éphémères, il semble qu'il y a trois types d'approches qui peuvent être utilisées pour établir une forme de propriété d'identité :

- Un tiers de confiance, qui déclare qu'une identité donnée est accessible à une ensemble de localisateurs donné, de sorte que le point d'extrémité atteint à un de ces localisateurs est le propriétaire de l'identité.

- Les identifiants fondés sur la cryptographie ou les adresses générées par cryptographie où la paire de clés publique/privée peut être utilisée pour prouver que l'identifiant a été généré par le nœud qui connaît la clé privée (ou par un autre nœud dont le hachage de clé publique a la même valeur).

- Un lien statique, comme actuellement défini dans IP, où on fait confiance au système d'acheminement pour livrer les paquets au propriétaire du localisateur, et comme le localisateur et l'identité sont un, on prouve la propriété de l'identité comme un sous produit.

Une solution aurait besoin de combiner des éléments qui fournissent la protection contre la redirection de communication à la fois préméditée et en cours. Cela peut être fait de plusieurs façons, et l'ensemble actuel de propositions ne paraît pas contenir toutes les combinaisons utiles. Par exemple, la propriété CBID de HIP pourrait être utilisée pour empêcher les attaques préméditées, tandis que les chaînes de hachage de WIMP pourraient être utilisées pour empêcher la redirection en cours. Et il y a probablement d'autres combinaisons intéressantes.

Un aspect en relation, mais peut-être séparé, est si la solution assure la protection contre les attaques par interposition avec des attaquants dans le chemin. Certains schémas, comme [HIP] et [NOID] le font, mais étant donné qu'un attaquant sur le chemin peut voir et modifier le trafic de données qu'il puisse ou non modifier la signalisation de multi-rattachements, ce niveau de protection semble exagéré. La protection contre un interposé sur le chemin pour le trafic de données peut être fait séparément en utilisant IPsec, TLS, etc.

Finalement, empêcher les attaques de DoS de tiers est conceptuellement plus simple ; il suffirait de vérifier d'une façon ou

d'une autre que l'homologue est bien joignable au nouveau localisateur avant d'envoyer un grand nombre de paquets à ce localisateur.

Tout comme les attaques de redirection sont conceptuellement empêchées en prouvant à un certain niveau la propriété de l'identifiant ou la propriété du contexte de communication, les attaques de Dos de tiers sont conceptuellement empêchées en montrant que le point d'extrémité est autorisé à utiliser un localisateur donné.

Les approches actuellement connues pour montrer une telle autorisation sont :

- L'acheminement de retour. C'est-à-dire, si un point d'extrémité est capable de recevoir des paquets à un localisateur donné, c'est parce que il est autorisé à le faire. Cela s'appuie sur le fait que l'acheminement est raisonnablement difficile à subvertir pour qu'il livre les paquets au mauvais endroit. Bien que cela pourrait être le cas quand les protocoles d'acheminement sont utilisés avec des mécanismes et pratiques de sécurité raisonnables, cela n'est pas le cas sur une seule liaison où ARP et la découverte de voisin peuvent être facilement falsifiés.

- Tiers de confiance. Un tiers établit qu'une identité donnée est autorisée à utiliser un ensemble donné de localisateurs (par exemple le DNS).

Adresse des auteurs

Erik Nordmark
Sun Microsystems, Inc.
17 Network Circle
Mountain View, CA 94025
USA
téléphone : +1 650 786 2921
mél : erik.nordmark@sun.com

Tony Li
mél : Tony.Li@tony.li

Déclaration complète de droits de reproduction

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