cheminement
**Request for Comments : 4593**
Catégorie : Information
Traduction Claude Brière de L'Isle

A. Barbir, Nortel
S. Murphy, Sparta, Inc.
Y. Yang, Cisco Systems
octobre 2006

# Menaces génériques contre les protocoles d'acheminement



**Résumé**
Les protocoles d'acheminement sont soumis à des attaques qui peuvent causer des dommages aux utilisateurs individuels ou au fonctionnement du réseau considéré dans son ensemble. Le présent document donne une description et un résumé des menaces génériques qui affectent les protocoles d'acheminement en général. Cet ouvrage décrit les menaces, y compris les sources et capacités de menace, les actions de menace et les conséquences des menaces, ainsi que celles d'une rupture des fonctions d'acheminement qui pourraient être attaquées séparément.

## Table des matières



## 1. Introduction

Les protocoles d'acheminement sont l'objet de menaces et d'attaques qui peuvent causer des dommages aux utilisateurs individuels ou au fonctionnement du réseau dans son ensemble. Le document fait un résumé des menaces génériques qui affectent les protocoles d'acheminement. En particulier, le présent travail identifie les menaces génériques pour les protocoles d'acheminement qui incluent des sources de menaces, des actions de menace, et des conséquences de menaces. Il fournit une analyse des interruptions des fonctions d'acheminement qui pourraient être attaquées séparément.

Ce travail devrait être considéré comme un précurseur du développement d'un ensemble commun d'exigences de sécurité pour les protocoles d'acheminement. Alors qu'il est bien connu qu'une mauvaise mise en œuvre, incomplète, ou défectueuse des protocoles d'acheminement, conduit par elle-même à des problèmes ou défaillances de l'acheminement ou peut augmenter le risque qu'un réseau soit attaqué avec succès, ces problèmes ne sont pas examinés ici. Le présent document considère seulement les attaques contre les mises en œuvre robustes, bien constituées, de protocoles d'acheminement, comme celles qui sont spécifiées dans le plus court chemin en premier (OSPF, *Open Shortest Path First*) [RFC2328], système intermédiaire à système intermédiaire (IS-IS, *Intermediate System to Intermediate System*) [RFC1195], [ISO10589], RIP [RFC2453] et BGP [RFC4271]. Les attaques contre les faiblesses et vulnérabilités spécifiques d'une mise en œuvre sortent du domaine d'application du présent document.

Le document est organisé comme suit : la Section 2 passe en revue les fonctions d'acheminement ; la Section 3 définit les menaces ; dans la Section 4, on discute les actions de menace généralement identifiables sur l'acheminement. La Section 5 traite des considérations sur la sécurité.

## 2. Vue d'ensemble des fonctions d'acheminement

Cette section donne une vue d'ensemble des fonctions courantes qui sont partagées par les divers protocoles d'acheminement. En général, les protocoles d'acheminement partagent les fonctions suivantes :

- Sous système de transport : le protocole d'acheminement transmet les messages à ses voisins en utilisant un protocole sous-jacent. Par exemple, OSPF utilise IP, tandis que d'autres protocoles peuvent fonctionner avec TCP.

- Maintenance de l'état de voisin : la formation des relations de voisinage est la première étape pour la détermination de la topologie. Pour cette raison, les protocoles d'acheminement peuvent avoir besoin de conserver les informations d'état. Chaque protocole d'acheminement peut utiliser un mécanisme différent pour déterminer ses voisins dans la topologie d'acheminement. Certains protocoles ont des échanges distincts par lesquels ils établissent les relations de voisinage, par exemple, les échanges de Hello dans OSPF.

- Maintenance de base de données : les protocoles d'acheminement échangent des informations sur la topologie du réseau et l'accessibilité. Les routeurs collectent ces informations dans les bases de données d'acheminement avec des détails variables. La maintenance de ces bases de données est une portion significative de la fonction d'un protocole d'acheminement.

Dans un protocole d'acheminement, il y a des échanges de messages qui sont destinés au contrôle de l'état du protocole. Par exemple, les messages de maintenance de voisin portent de telles informations. Par ailleurs, il y a des messages qui sont utilisés pour échanger des informations destinées à être utilisées dans la fonction de transmission, par exemple, les messages qui sont utilisés pour maintenir la base de données. Ces messages affectent la partie données (information) du protocole d'acheminement.

## 3. Modèle générique des menaces sur les protocoles d'acheminement

Le modèle développé dans cette section peut être utilisé pour identifier les menaces contre tout protocole d'acheminement.

Les protocoles d'acheminement sont l'objet de menaces à divers niveaux. Par exemple, les menaces peuvent affecter le sous système de transport, où le protocole d'acheminement peut être l'objet d'attaques contre son protocole sous-jacent. Un attaquant peut aussi attaquer les messages qui portent les informations de contrôle dans un protocole d'acheminement pour casser une relation de voisinage (par exemple, échange de trafic, adjacence). Ce type d'attaque peut impacter le comportement d'acheminement du réseau dans les routeurs affectés et probablement aussi le voisinage environnant. Par exemple, dans BGP, si un routeur reçoit un message CEASE, il va rompre ses relations de voisinage avec son homologue et potentiellement envoyer de nouvelles informations d'acheminement à tous les homologues restants.

Un attaquant peut aussi attaquer les messages qui portent des informations de données afin de casser un échange de base de données entre deux routeurs ou pour affecter la fonction de maintenance de la base de données. Par exemple, les informations de la base de données doivent être authentiques et autorisées. Un attaquant qui est capable d'introduire des données boguées peut avoir un fort effet sur le comportement d'acheminement dans le voisinage. Par exemple, si un routeur OSPF envoie des LSA avec le mauvais routeur annonceur, les receveurs vont calculer une arborescence de plus court chemin en premier (SPF, *Shortest Path First*) qui est incorrecte et peuvent ne pas transmettre le trafic. Si un routeur BGP annonce des informations d'accessibilité de couche réseau (NLRI, *Network Layer Reachability Information*) qu'il n'est pas autorisé à annoncer, les receveurs peuvent alors transmettre ce trafic de NLRI à ce routeur et le trafic ne pourra pas être livré. Un routeur de diffusion groupée indépendante du protocole (PIM, *Protocol Independent Multicast*) pourrait transmettre un message JOIN pour recevoir des données de diffusion groupée qu'il ne recevrait pas autrement.

### 3.1 Définitions de menaces

Dans la [RFC2828], une menace est définie comme un potentiel de violation de la sécurité, qui existe quand il y a des circonstances, capacités, actions, ou événements qui pourraient mettre en danger la sécurité et causer des dommages. Les

menaces peuvent être catégorisées comme des sources de menace, des actions de menace, des conséquences de menace, des zones de conséquence de menaces, et des périodes de conséquences de menaces.

### 3.1.1 Sources de menaces

Dans le contexte d'une attaque délibérée, une source de menace est définie comme un adversaire motivé et capable. En modélisant les motivations (buts de l'attaque) et les capacités des adversaires qui sont des sources de menace, on peut mieux comprendre quelles classes d'attaques ces menaces peuvent monter et donc quels types de contre-mesures vont être requis pour traiter ces attaques.

#### 3.1.1.1 Motivations des adversaires

On suppose que le but le plus courant d'un adversaire qui attaque délibérément l'acheminement est de causer un dysfonctionnement de l'acheminement inter domaines. Un dysfonctionnement de l'acheminement affecte la transmission de données de façon telle que le trafic suive un chemin (séquence de systèmes autonomes dans le cas de BGP) autre que celui qui aurait été calculé par le protocole d'acheminement si il fonctionnait correctement (c'est-à-dire, si il n'avait pas été attaqué). Par suite d'une attaque, une route peut se terminer sur un routeur autre que celui qui représente légitimement l'adresse de destination du trafic, ou elle peut traverser des routeurs autres que ceux qu'elle aurait traversé autrement. Dans l'un et l'autre cas, un dysfonctionnement de l'acheminement peut permettre à un adversaire d'espionner passivement le trafic, ou d'engager des attaques actives par interposition (MITM, *man-in-the-middle*) incluant d'éliminer du trafic (déni de service).

Un dysfonctionnement de l'acheminement peut être effectué pour un gain financier relatif au volume de trafic (par opposé au contenu du trafic acheminé) par exemple, pour affecter les règlements entre les FAI.

Un autre but possible des attaques contre l'acheminement peut être d'endommager l'infrastructure du réseau elle-même, sur une base ciblée ou à grande échelle. Donc, par exemple, des attaques qui causent une excessive transmission de messages UPDATE ou autres messages de gestion, et du traitement de routeur participant, pourrait être motivées par ces buts.

Sans considération des buts notés ci-dessus, un adversaire peut ou non être exposé à la détection et l'identification. Cette caractéristique d'un adversaire influence certaines des façons dont les attaques peuvent être réalisées.

#### 3.1.1.2 Capacités des adversaires

Les différents adversaires possèdent des capacités variées.

- Tous les adversaires sont présumés être capables de diriger les paquets sur des routeurs à partir de localisations distantes et peuvent affirmer une fausse adresse IP de source avec chaque paquet (usurpation d'adresse IP) dans un effort pour causer l'acceptation et le traitement du paquet par le routeur ciblé comme si il émanait de la source indiquée. Les attaques en usurpation peuvent être employées pour tromper les routeurs en les faisant agir sur des messages bogués pour effectuer un mauvais acheminement, ou ces messages peuvent être utilisés pour déborder le processeur de gestion dans un routeur, pour effectuer un déni de service. La protection contre de tels adversaires ne doit pas s'appuyer sur l'identité prétendue dans les paquets d'acheminement que le protocole reçoit.

- Certains adversaires peuvent surveiller les liaisons sur lesquelles du trafic d'acheminement est porté et émettre des paquets qui imitent les données contenues dans le trafic d'acheminement légitime porté sur ces liaisons ; donc, ils peuvent participer activement aux échanges de messages avec les routeurs légitimes. Cela augmente les opportunités pour un adversaire de générer du trafic d'acheminement bogué qui peut être accepté par un routeur, pour effectuer un changement d'acheminement ou du déni de service. La retransmission du trafic de gestion livré précédemment (attaque en répétition) sert d'exemple de cette capacité. Par suite, la protection contre de tels adversaires ne doit pas s'appuyer sur le secret de données non chiffrées dans les en-têtes ou les charges utiles de paquet.

- Certains adversaires peuvent effectuer des attaques par interposition (MITM) contre le trafic d'acheminement, par exemple, par suite d'un espionnage actif sur une liaison entre deux routeurs. Cela représente le sommet des capacités d'espionnage pour un adversaire. La protection contre de tels adversaires ne doit pas s'appuyer sur l'intégrité des liaisons inter routeurs pour authentifier le trafic, sauf si des mesures de chiffrement sont employées pour détecter une modification non autorisée.

- Certains adversaires peuvent subvertir les routeurs, ou les stations de travail de gestion utilisées pour contrôler ces routeurs. Ces défaillances byzantines représentent la forme la plus sérieuse de capacité d'attaque en ce qu'elles résultent en l'émission de trafic bogué par les routeurs légitimes. Par suite, la protection contre de tels adversaires ne doit pas compter sur le fonctionnement correct des routeurs du voisinage. Les mesures de protection devraient adopter le principe du moindre

privilège, pour minimiser l'impact d'attaques de cette sorte. Pour contrer les attaques byzantines, les routeurs ne devraient pas faire confiance au trafic de gestion (par exemple, sur la base de sa source) mais plutôt chaque routeur devrait authentifier de façon indépendante le trafic de gestion avant d'agir sur lui.

On supposera que toutes les contre mesures cryptographiques employées pour sécuriser BGP vont employer des algorithmes et modes résistants à l'attaque, même par des adversaires sophistiqués ; donc, on va ignorer les attaques de cryptanalyse.

Les attaques délibérées sont imitées par des défaillances aléatoires et non intentionnelles. En particulier, une défaillance byzantine dans un routeur peut se produire parce que le routeur est fautif dans son matériel ou son logiciel, ou est mal configuré. Comme décrit dans [Perlman], "Un nœud avec une défaillance byzantine peut corrompre les messages, falsifier les messages, retarder les messages, ou envoyer des messages contradictoires aux différents nœuds". Les routeurs byzantins, qu'ils soient fautifs, mal configurés, ou subvertis, ont le contexte pour fournir des informations d'acheminement boguées crédibles et très dommageables. Des routeurs byzantins peuvent aussi prétendre avoir l'identité d'un autre homologue légitime. Étant donné leur statut d'homologues, ils peuvent même éluder les protections d'authentification, si ces protections peuvent seulement détecter qu'une source est un des homologues légitimes (par exemple, le routeur utilise la même clé de chiffrement pour authentifier tous les homologues).

On caractérise donc les sources de menace en deux groupes :

Extérieur : cet attaquant peut résider n'importe où dans l'Internet, avoir la capacité d'envoyer du trafic IP au routeur, peut être capable d'observer les réponses du routeur, et peut même contrôler le chemin pour le trafic d'un homologue légitime. Ce n'est pas un participant légitime du protocole d'acheminement.

Byzantin : cet attaquant est un routeur fautif, mal configuré, ou subverti ; c'est-à-dire, un participant légitime au protocole d'acheminement.

### 3.1.2 Conséquences des menaces

Une conséquence de menace est une violation de la sécurité qui résulte d'une action de menace [RFC2828]. Pour un protocole d'acheminement, une violation de la sécurité est la compromission d'un aspect du comportement correct du système d'acheminement. La compromission peut endommager le trafic de données destiné à un réseau ou hôte particulier ou peut endommager le fonctionnement de l'infrastructure d'acheminement du réseau dans son ensemble.

Il y a quatre types de conséquences générales de menace : divulgation, tromperie, interruption, et usurpation [RFC2828].

- Divulgation : la divulgation d'informations d'acheminement se produit quand un attaquant réussit à accéder aux informations sans y être autorisé. Les extérieurs qui peuvent observer ou surveiller une liaison peuvent causer la divulgation, si les échanges d'acheminement n'ont pas de protection de confidentialité. Les routeurs byzantins peuvent causer la divulgation, pour autant qu'ils soient bien impliqués dans les échanges d'acheminement. Bien qu'une divulgation inappropriée des informations d'acheminement puisse faire peser une menace de sécurité ou faire partie d'une attaque ultérieure, plus large, ou de couche supérieure, la confidentialité n'est généralement pas un but de la conception des protocoles d'acheminement.

- Tromperie : cette conséquence apparaît quand un routeur légitime reçoit un message d'acheminement falsifié et croit qu'il est authentique. Les routeurs extérieurs et byzantins peuvent causer cette conséquence si le routeur receveur n'a pas la capacité de vérifier l'intégrité ou d'authentifier l'origine des messages d'acheminement.

- Interruption : cette conséquence se produit quand le fonctionnement d'un routeur légitime est interrompu ou empêché. Un extérieur peut causer cela en insérant, corrompant, répétant, retardant, ou éliminant les messages d'acheminement, ou en cassant les sessions d'acheminement entre les routeurs légitimes. Les routeurs byzantins peuvent causer cette conséquence en envoyant de faux messages d'acheminement, interférant avec les échanges normaux d'acheminement, ou en inondant de messages inutiles de protocole d'acheminement. (Le déni de service est une action de menace courante qui cause l'interruption.)

- Usurpation : cette conséquence survient quand un attaquant obtient le contrôle sur les services/fonctions qu'un routeur légitime fournit aux autres. Les extérieurs peuvent causer cela en retardant ou en éliminant des échanges d'acheminement, ou en fabriquant ou répétant des informations d'acheminement. Les routeurs byzantins peuvent causer cette conséquence en envoyant de fausses informations d'acheminement ou en interférant avec les échanges d'acheminement.

Note : un attaquant n'a pas à avoir le contrôle direct d'un routeur pour contrôler ses services. Par exemple, dans la Figure 1, le réseau N 1 a un double rattachement par les routeurs Rtr A et Rtr B, et Rtr A est préféré. Cependant, Rtr B est compromis et annonce une meilleure métrique. Par conséquent, les appareils sur l'Internet choisissent le chemin par Rtr B pour atteindre N 1. De cette façon, le routeur B vole le trafic de données, et le routeur A perd son contrôle des services au routeur B. C'est ce que décrit la Figure 1.

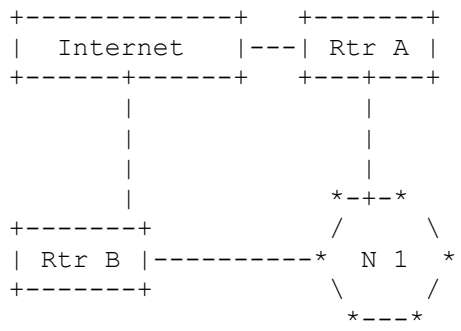


**Figure 1. Réseau à double rattachement**

Plusieurs conséquences de menace peuvent être causées par une seule action de menace. Dans la Figure 1, il existe au moins deux conséquences : les routeurs qui utilisent Rtr B pour accéder à N 1 sont trompés, et Rtr A est usurpé.

#### 3.1.2.1 Portée des conséquences de menaces

Comme mentionné ci-dessus, une attaque peut endommager le trafic de données destiné à un réseau ou hôte particulier ou endommager le fonctionnement de l'infrastructure d'acheminement du réseau dans son ensemble. Les dommages qui peuvent résulter des attaques contre le réseau dans son ensemble peuvent inclure :

- L'encombrement du réseau. Plus de trafic de données est transmis sur une portion du réseau qu'il serait autrement nécessaire pour porter le trafic.
- Trou noir. De grandes quantités de trafic sont inutilement redirigées pour être transmises à travers un routeur et ce routeur élimine de nombreux paquets, ou la plupart, ou tous.
- Boucle. Le trafic de données est transmis le long d'une route en boucle, de sorte que les données ne sont jamais livrées (résultant en l'encombrement du réseau).
- Partition. Une certaine portion du réseau croit qu'elle est séparée du reste du réseau, alors qu'elle ne l'est pas.
- Bouillonnement *(churn)*. La transmission dans le réseau change (inutilement) à un rythme rapide, résultant en de grandes variations des schémas de livraison des données (et affectant les techniques de contrôle de l'encombrement).
- Instabilité. Le protocole devient instable de sorte que la convergence à un état de transmission global n'est pas réalisée.
- Sur contrôle. Les messages du protocole d'acheminement deviennent eux-mêmes une portion significative du trafic que pote le réseau.
- Entrave *(clog)*. Un routeur reçoit un nombre excessif de messages de protocole d'acheminement, causant l'épuisement de certaines ressources (par exemple, mémoire, CPU, batterie).

Les dommages qui peuvent résulter d'attaques contre une adresse d'hôte ou de réseau particulière peuvent inclure :

- La famine. Le trafic de données destiné au réseau ou hôte est transmis à une partie du réseau qui ne peut pas le livrer.
- Espionnage. Le trafic de données est transmis par un routeur ou réseau qui autrement ne verrait pas ce trafic, donnant une opportunité de voir les données ou au moins le schéma de livraison des données.
- Coupure. Une portion du réseau croit qu'il n'y a pas de route pour l'hôte ou réseau alors qu'il est en fait connecté.

- o Retard. Le trafic de données destiné au réseau ou hôte est transmis sur une route qui est d'une certaine façon inférieure à celle qu'il aurait prise autrement.

- o Boucle. Le trafic de données pour le réseau ou hôte est transmis sur une route en boucle, de sorte qu'il n'est jamais livré.

Il est important de considérer toutes les conséquences, parce que certaines solutions de sécurité peuvent protéger contre une conséquence mais pas contre les autres. Il est possible de concevoir une solution de sécurité qui protège contre l'espionnage le trafic d'une destination sans protéger contre le bouillonnement dans le réseau. De même, il est possible de concevoir une solution de sécurité qui empêche une attaque de famine contre un hôte, mais pas contre une attaque d'entrave contre un routeur. Les exigences de sécurité doivent être claires sur quelles conséquences sont évitées, et quelles conséquences doivent être traitées par d'autres moyens (par exemple, des moyens administratifs hors du protocole).

#### 3.1.2.2 Zone de conséquences de menace

Une zone de conséquences de menace couvre la zone au sein de laquelle les opérations du réseau ont été affectées par des actions de menace. Les zones possibles de conséquences de menaces peuvent être classées comme une seule liaison ou routeur, plusieurs routeurs (au sein d'un seul domaine d'acheminement) un seul domaine d'acheminement, plusieurs domaines d'acheminement, ou l'Internet global. La zone de conséquences de menace varie sur la base de l'action de menace et de la position de la cible de l'attaque. Des actions de menace similaires qui arrivent en des localisations différentes peuvent résulter en des zones de conséquences de menace totalement différentes. Par exemple, quand un extérieur casse la session d'acheminement entre un routeur de distribution et un routeur d'extrémité, seule l'accessibilité de et vers les appareils du réseau rattachés au routeur d'extrémité vont être impactés. En d'autres termes, la zone de conséquences de menace est un seul routeur. Dans un autre cas, si l'extérieur est situé entre un routeur de bordure de consommateur et son routeur bordure de fournisseur correspondant, une telle action peut causer la perte de la connexion de tout le site du consommateur. Dans ce cas, la zone de conséquences de menace pourrait être un seul domaine d'acheminement.

#### 3.1.2.3 Période de conséquences de menace

Une période de conséquences de menace est définie comme la portion de temps durant laquelle les opérations du réseau sont impactées par les conséquences de menace. La période de conséquences de menace est influencée par la durée de l'action de menace, mais n'en dépend pas totalement. Dans certains cas, les opérations du réseau vont revenir à la normale aussitôt que l'action de menace a été arrêtée. Dans d'autres cas, cependant, les conséquences de menace peuvent persister plus longtemps que l'action de menace. Par exemple, dans l'algorithme original d'état de liaison du réseau de l'agence pour les projets de recherche avancés (ARPANET, *Advanced Research Projects Agency Network*) certaines erreurs dans un routeur introduisaient trois instances d'une annonce d'état de liaison (LSA, *Link-State Announcement*). Elles s'écoulaient toutes à travers le réseau en continu, jusqu'à ce que le réseau entier soit parcouru [RFC0789].

## 4. Actions de menaces sur l'acheminement généralement identifiables

Cette section traite des actions de menace généralement identifiables et reconnues contre les protocoles d'acheminement. Les actions de menace ne sont pas nécessairement spécifiques de protocoles individuels mais peuvent être présentes dans un ou plusieurs des protocoles d'acheminement courants utilisés actuellement.

### 4.1 Exposition délibérée

L'exposition délibérée quand un attaquant prend le contrôle d'un routeur et délivre intentionnellement des informations d'acheminement à d'autres entités (par exemple, l'attaquant, une page de la Toile, un message électronique ou un autre routeur) qui autrement ne devrait pas recevoir les informations exposées.

La conséquence de l'exposition délibérée est la divulgation des informations d'acheminement.

La zone de conséquences de menace de l'exposition délibérée dépend des informations d'acheminement que les attaquants ont exposées. Plus les connaissances sont exposées, plus la zone de conséquences de menace est grande.

La période de conséquences de menace de l'exposition délibéré peut être plus longue que la durée de l'action elle-même. Les informations d'acheminement exposées ne seront pas périmées avant qu'il y ait un changement de topologie du réseau exposé.

### 4.2 Reniflage

Le reniflage est une action par laquelle des attaquants surveillent et/ou enregistrent les échanges d'acheminement entre des routeurs autorisés pour capturer les informations d'acheminement. Les attaquants peuvent aussi capturer les informations de trafic de données (cependant, ceci sort du domaine d'application de ce document).

La conséquence du reniflage est la divulgation des informations d'acheminement.

La zone de conséquences de menace du reniflage dépend de la localisation de l'attaquant, du type de protocole d'acheminement, et des informations d'acheminement qui ont été enregistrées. Par exemple, si l'extérieur renifle une liaison qui est dans une zone OSPF totalement d'extrémité ; la zone de conséquences de menace devrait être limitée à la zone entière. Un attaquant qui renifle une liaison dans une session du protocole de routeur bordure externe (EBGP, *External Border Gateway Protocol*) peut obtenir la connaissance de plusieurs domaines d'acheminement.

La période de conséquences de menace peut être plus longue que la durée de l'action. Si un attaquant arrête de renifler une liaison, les connaissances acquises ne seront pas périmées avant qu'il y ait un changement de topologie du réseau affecté.

### 4.3 Analyse de trafic

L'analyse de trafic est une action par laquelle des attaquants obtiennent des informations d'acheminement en analysant les caractéristiques du trafic de données sur une liaison subvertie. Les menaces d'analyse de trafic peuvent affecter toutes les données qui sont envoyées sur une liaison de communication. Cette menace n'est pas particulière aux protocoles d'acheminement et est incluse ici par souci de complétude.

La conséquence d'une analyse de trafic de données est la divulgation des informations d'acheminement. Par exemple, les adresses IP de source et de destination du trafic de données et le type, la magnitude, et le volume du trafic peuvent être divulgués.

La zone de conséquences de menace de l'analyse de trafic dépend de la localisation de l'attaquant et de quel trafic de données est passé. Un attaquant du cœur de réseau devrait être capable de collecter plus d'informations que son équivalent sur les bordures et va donc être capable d'analyser les schémas de trafic dans une plus large zone.

La période de conséquences de menace peut être plus longue que la durée de l'analyse de trafic. Après que l'attaquant a arrêté l'analyse de trafic, ses connaissances ne seront pas périmées tant qu'il n'y aura pas de changement de topologie du réseau divulgué.

### 4.4 Usurpation

L'usurpation survient quand un appareil illégitime prend l'identité d'un appareil légitime. L'usurpation n'est souvent par elle-même pas la vraie attaque. L'usurpation est particulière en ce qu'elle peut être utilisée pour réaliser d'autres actions de menace causant d'autres conséquences de menace. Un attaquant peut utiliser l'usurpation comme moyen de lancer d'autres types d'attaques. Par exemple, si un attaquant réussit à usurper l'identité d'un routeur, il peut envoyer des informations d'acheminement fantaisistes qui peuvent causer l'interruption des services du réseau.

Il y a peu de cas où une usurpation peut être une attaque en et par elle-même. Par exemple, les messages provenant d'un attaquant qui usurpe l'identité d'un routeur légitime peuvent causer la formation d'une relation de voisinage et empêcher la formation de la relation avec le routeur légitime.

Les conséquences de l'usurpation sont les suivantes :

- Divulgation des informations d'acheminement. Le routeur usurpateur va être capable d'obtenir l'accès aux informations d'acheminement.
- Rupture de la relation d'homologue. Les routeurs autorisés, qui échangent des messages d'acheminement avec le routeur usurpateur, ne réalisent pas qu'ils voisinent avec un routeur qui a usurpé l'identité d'un autre routeur.

La zone de conséquences de menace est la suivante :

- La zone de conséquences de la fausse relation d'homologue va être limitée aux routeurs qui font confiance à l'identité revendiquée par l'attaquant.
- La zone de conséquences des informations d'acheminement divulguées dépend de la localisation de l'attaquant, du type de protocole d'acheminement, et des informations d'acheminement qui ont été échangées entre l'attaquant et ses voisins trompés.

Note : ce paragraphe se concentre sur l'usurpation d'adressage comme une menace en propre. Cependant, l'usurpation crée des conditions pour d'autres actions de menaces. Les autres actions de menace sont considérées comme des falsifications et sont traitées dans le paragraphe suivant.

### 4.5 Falsification

La falsification est une action par laquelle un attaquant envoie de fausses informations d'acheminement. Pour falsifier les informations d'acheminement, un attaquant doit être soit le générateur, soit un transmetteur des informations d'acheminement. Il ne peut pas être seulement un receveur. Les fausses informations d'acheminement décrivent le réseau d'une façon non réaliste, qu'elles soient ou non prévues par l'administrateur de réseau qui a l'autorité pour le faire.

#### 4.5.1 Falsifications par l'origine

Un générateur d'informations d'acheminement peut lancer les falsifications décrites dans les paragraphes suivants.

##### 4.5.1.1 Prétentions injustifiées

Des prétentions injustifiées se produisent quand un routeur byzantin ou un extérieur annonce son contrôle sur des ressources du réseau, alors qu'en réalité il ne l'a pas, ou si l'annonce n'est pas autorisée. C'est ce que montrent les Figures 2 et 3.

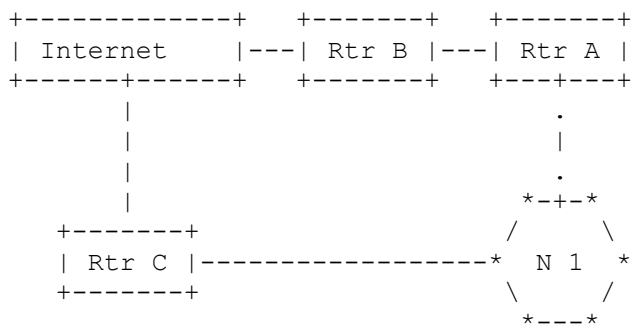


**Figure 2. Prétentions injustifiées 1**

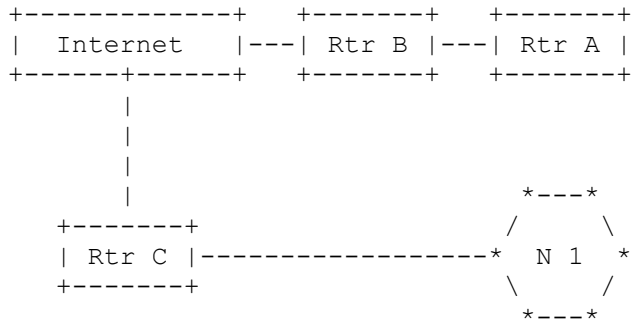


**Figure 3. Prétentions injustifiées 2**

Les figures ci-dessus donnent des exemples de prétentions injustifiées. Le routeur A, l'attaquant, est connecté à l'Internet par le routeur B. Le routeur C est autorisé à annoncer sa liaison au réseau 1. Dans la Figure 2, le routeur A contrôle une liaison au réseau 1 mais n'est pas autorisé à l'annoncer. Dans la Figure 3, le routeur A ne contrôle pas une telle liaison. Mais dans l'un et l'autre cas, le routeur A annonce la liaison à l'Internet, à travers le routeur B.

Les routeurs byzantins et les extérieurs peuvent émettre des prétentions injustifiées sur des ressources du réseau. les conséquences des prétentions injustifiées incluent ce qui suit :

- Usurpation des ressources du réseau faisant l'objet des prétentions injustifiées. Dans les Figures 2 et 3, l'usurpation du réseau 1 peut survenir quand le routeur B (ou d'autres routeurs sur l'Internet non montrés dans les figures) croit que le routeur A fournit le meilleur chemin pour atteindre le réseau 1. Par suite, les routeurs transmettent le trafic de données destiné au réseau 1 au routeur A. Le meilleur résultat est que le trafic de données utilise un chemin non autorisé, comme

dans la Figure 2. Le pire cas est que les données n'atteignent jamais la destination du réseau 1, comme dans la Figure 3. La conséquence ultime est que le routeur A gagne le contrôle sur les services du réseau 1, en contrôlant le trafic de données.

- o Usurpation des routeurs annonceurs légitimes. Dans les Figures 2 et 3, le routeur C est l'annonceur légitime du réseau. Par ses prétentions injustifiées, le routeur A contrôle aussi (en partie ou en totalité) les services/fonctions fournis par le routeur C. (Ce N'est PAS une interruption, car le routeur C est en fonction de la façon prévue par l'administrateur d'autorité du réseau.)
- o Tromperie des autres routeurs. Dans les Figures 2 et 3, le routeur B, ou les autres routeurs sur l'Internet, peuvent être trompés et croire que le chemin à travers le routeur A est le meilleur.
- o Interruption des plans de données sur certains routeurs. Cela peut arriver aux routeurs qui sont sur le chemin utilisé par d'autres routeurs pour atteindre les ressources usurpées du réseau à travers l'attaquant. Dans les Figures 2 et 3, quand d'autres routeurs sur l'Internet sont trompés, ils vont transmettre le trafic de données au routeur B, qui pourrait être surchargé.

La zone de conséquences de menace varie sur la base des conséquences :

- o Lorsque l'usurpation est concernée, la zone de conséquences couvre les ressources du réseau qui sont l'objet de prétentions injustifiées de la part de l'attaquant (réseau 1 dans les Figures 2 et 3) et les routeurs qui sont autorisés à annoncer les ressources du réseau mais perdent la compétition contre l'attaquant (routeur C dans les Figures 2 et 3).
- o Lorsque la tromperie est concernée, la zone de conséquences couvre les routeurs qui croient aux annonces de l'attaquant et utilisent l'attaquant pour atteindre les réseaux visés (routeur B et autres routeurs trompés dans l'Internet dans les Figures 2 et 3).
- o Lorsque l'interruption est concernée, la zone de conséquences inclut les routeurs qui sont sur le chemin du trafic de données mal dirigé (routeur B dans les Figures 2 et 3 et autres routeurs dans l'Internet sur le chemin du trafic mal dirigé).

La conséquence de la menace ne va pas cesser quand l'attaquant arrête ses prétentions injustifiées et ne va totalement disparaître que quand les tableaux d'acheminement vont converger. Par suite, la période de conséquences est plus longue que la durée des prétentions injustifiées .

#### 4.5.1.2 Revendication à tort

Une menace de revendication à tort est définie comme une action par laquelle un attaquant annonce des ressources du réseau qu'il est autorisé à contrôler, mais d'une façon qui n'est pas conforme aux intentions de l'administrateur qui a autorité sur le réseau. Par exemple, il peut annoncer des coûts de liaison inappropriés dans une LSA OSPF. Un attaquant peut faire l'éloge ou déprécier des ressources du réseau dans ses annonces. Les routeurs byzantins peuvent revendiquer à tort des ressources du réseau.
Les conséquences de menace de la revendication à tort sont similaires aux conséquences des prétentions injustifiées.
La zone de conséquence et sa période sont aussi similaires à celles des prétentions injustifiées.

### 4.5.2 Falsifications par les transmetteurs

Dans chaque protocole d'acheminement, les routeurs qui transmettent des messages de protocole d'acheminement sont supposés laisser certains champs non modifiés et modifier d'autres champs de certaines façons circonscrites. Les champs à modifier, les nouveaux contenus possibles de ces champs et leur calcul à partir des champs d'origine, les champs qui doivent rester non modifiés, etc. sont tous détaillés dans la spécification du protocole. Ils peuvent varier selon la fonction du routeur ou son environnement de réseau. Par exemple, dans RIP, le transmetteur doit modifier les informations d'acheminement en augmentant de 1 le compte de bonds. Par ailleurs, un transmetteur ne doit pas modifier de champ de LSA de type 1 dans OSPF sauf le champ Age. En général, les transmetteurs des protocoles d'acheminement en vecteur de distance sont autorisés à, et doivent modifier les informations d'acheminement, tandis que la plupart des transmetteurs des protocoles d'acheminement en état de liaison ne sont pas autorisés à, et ne doivent pas modifier la plupart des informations d'acheminement.

Comme transmetteur autorisé à modifier les messages d'acheminement, un attaquant pourrait aussi falsifier en ne transmettant pas comme exigé les informations d'acheminement aux autres routeurs autorisés.

#### 4.5.2.1 Fausses déclarations

Ceci est défini comme une action par laquelle l'attaquant modifie les attributs de chemin d'une manière incorrecte. Par exemple, dans RIP, l'attaquant pourrait augmenter le coût du chemin de deux bonds au lieu d'un. Dans BGP, l'attaquant pourrait supprimer certains numéros d'AS du AS PATH.

Lorsque la transmission des informations d'acheminement ne devrait pas être modifiée, un attaquant peut lancer les falsifications suivantes :

- o Suppression. L'attaquant supprime des données valides dans le message d'acheminement.
- o Insertion. L'attaquant insère de fausses données dans le message d'acheminement.
- o Substitution. L'attaquant remplace des données valides dans le message d'acheminement par de fausses données.

Un transmetteur peut aussi falsifier des données en répétant des données périmées dans le message d'acheminement comme étant les données actuelles.

Tous les types d'attaquants, extérieurs et routeurs byzantins, peuvent falsifier les informations d'acheminement quand ils transmettent les messages d'acheminement.

Les conséquences de menace de ces falsifications par les transmetteurs sont similaires à celles causées par les générateurs : usurpation de certaines ressources du réseau et des routeurs en rapport ; tromperie des routeurs en utilisant de faux chemins ; et interruption des plans de données des routeurs sur les faux chemins. La zone de conséquences de menace et la période sont aussi similaires.

### 4.6 Interférence

L'interférence est une action de menace par laquelle un attaquant inhibe les échanges des routeurs légitimes. L'attaquant peut le faire en ajoutant du bruit, en ne transmettant pas les paquets, en répétant des paquets périmés, en insérant ou corrompant les messages, en retardant les réponses, en refusant les accusés de réception, ou en rompant la synchronisation.

Les routeurs byzantins peuvent ralentir leurs échanges d'acheminement ou induire du flottement dans les sessions d'acheminement de routeurs voisins légitimes.

La conséquence de l'interférence est l'interruption des opérations d'acheminement.

La zone de conséquence de l'interférence dépend de la sévérité de l'interférence. Si l'interférence résulte en des conséquences au niveau de la maintenance de voisin, il peut alors y avoir des changements dans la base de données, résultant en conséquences au niveau du réseau.

Les conséquences de menace pourraient disparaître aussitôt que l'interférence est arrêtée ou pourraient ne pas totalement disparaître avant que les réseaux n'aient convergé. Donc, la période de conséquence est égale ou plus longue que la durée de l'interférence.

### 4.7 Surcharge

La surcharge est définie comme une action de menace par laquelle des attaquants font peser une charge excessive sur les routeurs légitimes. Par exemple, il est possible à un attaquant de déclencher chez un routeur la création d'une quantité d'état excessive que les autres routeurs dans le réseau ne seront pas capables de traiter. De façon similaire, il est possible qu'un attaquant surcharge les échanges d'acheminement de la base de données et donc influence les opérations d'acheminement.

## 5. Considérations sur la sécurité

Ce document est entièrement consacré à la sécurité. Spécifiquement, le document traite de la sécurité des protocoles d'acheminement en tant qu'associée aux menaces sur ces protocoles. Dans un contexte plus large, ce travail s'appuie sur la reconnaissance par la communauté de l'IETF que la signalisation et les plans de contrôle/gestion des appareils de l'inter réseautage ont besoin d'être renforcés. Les protocoles d'acheminement peuvent être considérés comme faisant partie du plan de signalisation et contrôle. Cependant, aujourd'hui, les protocoles d'acheminement sont largement restés non protégés et ouverts aux attaques malveillantes. Le présent document discute les menaces contre les protocoles d'acheminement inter et intra domaine qui sont actuellement connues et pose les fondations pour d'autres documents qui vont discuter les exigences de sécurité pour les protocoles d'acheminement. Le présent document est indépendant des protocoles.

## 6. Références pour information

[ISO10589] ISO 10589, "Intermediate System to Intermediate System intra-domain routeing information exchange protocol for use in conjunction with the protocol for providing the connectionless-mode network service (ISO 8473)", ISO/IEC 10589:2002.

[Perlman] Perlman, R., "Network Layer Protocols with Byzantine Robustness", thèse de doctorat, MIT LCS TR-429, octobre 1988.

[RFC0789] E. Rosen, "Faiblesses des protocoles de commande du réseau : un exemple", juillet 1981.

[RFC1195] R. Callon, "Utilisation de l'IS-IS OSI pour l'acheminement dans les environnements TCP/IP et duels", décembre 1990. *(Mise à jour par les* RFC 1349, 5302, 5304*)*

[RFC2328] J. Moy, "OSPF version 2", STD 54, avril 1998. *(MàJ par la* RFC6549, RFC8042)

[RFC2453] G. Malkin, "RIP version 2", STD 56, novembre 1998. *(Mise à jour par la RFC* 4822*)*

[RFC2828] R. Shirey, "Glossaire de la sécurité sur l'Internet", FYI 36, mai 2000. (*Obsolète, voir* RFC4949)

[RFC4271] Y. Rekhter, T. Li et S. Hares, "Protocole de routeur frontière version 4 (BGP-4)", janvier 2006. *(D.S.) (MàJ par* RFC6608, RFC8212)

## Appendice A. Remerciements

Le présent document n'aurait pas éé possible sans les excellents efforts et l'esprit d'équipe de Dennis Beard, Nortel ; Ayman Musharbash, Nortel ; Jean-Jacques Puig, int-evry, France ; Paul Knight, Nortel ; Elwyn Davies, Nortel ; Ameya Dilip Pandit, étudiant diplômé, University of Missouri ; Senthilkumar Ayyasamy, étudiant diplômé, University of Missouri ; Stephen Kent, BBN ; Tim Gage, Cisco Systems ; James Ng, Cisco Systems ; Alvaro Retana, Cisco Systems.

## Appendice B. Acronymes

AS *(Autonomous System)* système autonome : ensemble de routeurs sous une seule administration technique. Chaque AS utilise normalement un seul protocole de passerelle intérieure (IGP) et sa métrique pour propager les informations d'acheminement au sein de l'ensemble de routeurs. Aussi appelé domaine d'acheminement.

Chemin d'AS : dans BGP, le chemin pour une destination. Le chemin consiste en les numéros d'AS de tous les routeurs qu'un paquet doit traverser pour atteindre une destination.

BGP *(Border Gateway Protocol)* : protocole de passerelle frontière. C'est le protocole de passerelles extérieures utilisé pour échanger les informations d'acheminement entre les routeurs des différents systèmes autonomes.

LSA *(Link-State Announcement)* : annonce d'état de liaison.

NLRI *(Network Layer Reachability Information)* : Informations d'accessibilité de couche réseau ; elles sont portées dans les paquets BGP et sont utilisées par MBGP.

OSPF *(Open Shortest Path First)* : plus court chemin ouvert en premier. IGP d'état de liaison qui prend les décisions d'acheminement sur la base de l'algorithme de plus court chemin d'abord (SPF, *shortest-path-first*) (aussi appelé algorithme de Dijkstra).

**Adresse des auteurs**

Abbie Barbir
Nortel
3500 Carling Avenue
Nepean, Ontario K2H 8E9
Canada
mél : abbieb@nortel.com

Sandy Murphy
Sparta, Inc.
7110 Samuel Morse Drive
Columbia, MD
USA
mél : sandy@sparta.com

Yi Yang
Cisco Systems
7025 Kit Creek Road
RTP, NC 27709
USA
mél : yiya@cisco.com

## Déclaration complète de droits de reproduction



**Remerciement**

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