Sécurisation du routage pour les décideurs politiques : un livre blanc de l'Internet Society

Octobre 2018

Bien qu'invisible aux yeux des utilisateurs moyens, le routage du protocole Internet (IP) soutient Internet. En veillant à ce que les paquets[1] aillent où ils sont censés aller, le routage[2] joue un rôle central dans le fonctionnement fiable de l'Internet. Il garantit que les e-mails parviennent aux bons destinataires, que les sites de commerce électronique demeurent opérationnels et que les services du gouvernement virtuel continuent à servir les citoyens. La sécurité du système de routage mondial est essentielle à la croissance continue de l'Internet et pour garantir les opportunités qu'il offre à tous les utilisateurs.

Chaque année, des milliers d'incidents de routage[3] se produisent, chacun ayant le potentiel de nuire à la confiance des utilisateurs et d'entraver le potentiel de l'Internet.[4] Ces incidents de routage peuvent aussi créer de réels dommages économiques. Les services clés peuvent devenir indisponibles, perturbant la capacité des entreprises et des utilisateurs à participer au commerce électronique.[5] Ou les paquets peuvent être détournés vers des réseaux malveillants, offrant la possibilité de les espionner.[6] Bien que des mesures de sécurité connues puissent régler nombre de ces incidents de routage, des incitations incompatibles en limitent l'usage.

Toutes les parties prenantes, y compris les décideurs politiques, doivent entreprendre des efforts pour renforcer la sécurité du système de routage mondial.[7] Cela ne peut uniquement être fait qu'en préservant en même temps les aspects vitaux du système de routage qui ont permis à Internet d'être

1 Les paquets de réseaux, ou « paquets » sont des données envoyées en utilisant un ou des réseaux.

2 Le routage est la pratique de détermination du moyen de transporter les données d'un endroit à un autre par un ou des réseaux

3 Les incidents de routage sont des mises à jour du Border Gateway Protocol qui ont un impact négatif.

4 https://www.internetsociety.org/blog/2018/01/14000-incidents-2017-routing-security-year-review/

5 Par exemple, en avril 2017, une fuite de route a causé une « interruption à grande échelle qui a freiné ou bloqué l'accès à des sites Web et des services en ligne pour des dizaines de sociétés japonaises. » https://bgpmon.net/bgp-leak-causing-internet-outages-in-japan-and-beyond/

6 Pendant plusieurs minutes en avril 2017, un opérateur de réseau suspect a détourné le trafic Internet de plusieurs services financiers. Si c'était intentionnel, le détournement aurait pu servir à donner la possibilité à l'opérateur de réseau de lire des informations financières non cryptées lors du passage sur son réseau, ou d'essayer de décrypter les informations financières cryptées. https://arstechnica.com/information-technology/2017/04/russian-controlled-telecom-hijacks-financial-services-internet-traffic/

7 Bien que les autres formes de sécurité (p.ex. la sécurité physique ou la sécurité des données) sont importantes pour l'ensemble des parties prenantes, y compris les opérateurs de réseau, ce document de politique générale est conçu pour se concentrer uniquement sur l'amélioration de la sécurisation du routage. Pour plus d'information sur la façon de sécuriser l'infrastructure des fournisseurs de services Internet, veuillez consulter : https://www.rfc-editor.org/rfc/rfc3871.txt

si omniprésent et améliorer sa sécurité. En donnant l'exemple dans leurs propres réseaux, en renforçant la communication et en participant à l'amélioration des incitations pour renforcer la sécurité, les décideurs politiques peuvent contribuer à améliorer l'écosystème de la sécurisation du routage.

Principales considérations

Le système de routage repose en son centre sur la confiance entre les réseaux. Le système de routage mondial est un système complexe, décentralisé, composé de dizaines de milliers de réseaux individuels. Des décisions commerciales indépendantes et des relations de confiance entre les opérateurs de réseaux individuels mettant en œuvre le Border Gateway Protocol (abréviation BGP) déterminent la façon dont le réseau se comporte.[8] L'architecture maillée du réseau contribue à sa résilience, son extensibilité et la facilité de son adoption.

Sans point de panne unique ou contrôleur unique, le système de routage est difficile à rompre au niveau mondial, de connexion facile et se dimensionne bien. Lorsqu'une route devient embouteillée ou échoue, les réseaux peuvent choisir de router le trafic en évitant les zones problématiques. La structure du système de routage permet aussi aux opérateurs de réseau une grande souplesse dans le fonctionnement de leurs propres réseaux. Elle permet aux opérateurs de réseau de développer de nouvelles architectures réseau et solutions pour coller le mieux aux besoins de leurs utilisateurs. Ce sont ces qualités qui ont rendu Internet si prospère et lui ont permis cette croissante.

Défis

Bien que les qualités du système de routage lui aient permis son succès global, ces mêmes attributs ont aussi contribué à certains de ses défis. Le système est fondé sur des liens de confiance ; chaque réseau compte sur les réseaux voisins (qui à leur tour comptent sur leurs propres voisins, etc.) pour agir de manière appropriée. Aucune vérification n'est intégrée et faire de fausses déclarations peut être facile. Cela conduit régulièrement à des **incidents de routage**. Les complexités et la décentralisation du système de routage mondial créent aussi **des défis pour l'écosystème**, y compris des incitations incompatibles et des risques externalisés posés par l'insécurité du routage. Les solutions pour gérer ces nombreux incidents de routage sont connues, mais les défis de l'écosystème gênent leur mise en œuvre. Tout effort pour atténuer ces défis doit reconnaître les fonctions techniques centrales du système de routage et maintenir les bénéfices offerts par son architecture.

En 2017, près de 14 000 incidents de routage ont été enregistrés.[9] Ces incidents ont affecté plus de 10 % des systèmes autonomes (AS) de l'Internet. Il y a trois grands types d'incidents de routage :

- **L'usurpation d'identité numérique,** lorsqu'un opérateur de réseau ou un pirate usurpe l'identité d'un autre opérateur de réseau, en prétendant que c'est le chemin correct vers le serveur ou le réseau recherché sur Internet.[10]

8 Un *protocole de routage* est la façon par laquelle un réseau détermine le chemin qu'un paquet de données doit prendre. Pour acheminer le trafic entre les réseaux, ceux-ci utilisent le Border Gateway Protocol (BGP).

9 https://www.internetsociety.org/blog/2018/01/14000-incidents-2017-routing-security-year-review/

10 Dans un cas d'usurpation d'identité numérique, un opérateur de réseau ou un attaquant usurpe l'identité d'un autre opérateur de réseau, en prétendant que c'est le chemin correct vers le serveur ou le réseau recherché sur Internet. Cela cause l'envoi de paquets au mauvais endroit, des attaques de déni de service (DoS) ou une interception du trafic.

- **Les fuites de route,** représentent la propagation d'annonces de routage[11] au-delà de leur portée prévue (en violation de leurs politiques).[12,13]

- **L'usurpation d'adresse IP,** lorsque quelqu'un crée des paquets IP avec une fausse adresse IP d'origine pour dissimuler l'identité de l'expéditeur ou usurper l'identité d'un autre système.[14]

Ces incidents peuvent provoquer une tension importante de l'infrastructure, résultant en un abandon de trafic, fournissant les moyens d'une inspection de trafic, ou même pouvant être utilisés pour réaliser des attaques d'amplification du serveur du nom de domaine (DNS),[15] ou d'autres attaques d'amplification réflective (RA).[16]

Les meilleures pratiques de sécurisation du routage sont déjà disponibles et sont considérées comme très efficaces contre ces formes d'incidents de routage. Pour les fuites de route comme pour les usurpations d'identité numérique, les réseaux peuvent utiliser des politiques de filtrage plus robustes[17] pour déterminer si de fausses annonces sont faites par les réseaux voisins. La validation de l'origine de l'IP[18] peut être utilisée pour localiser le trafic détourné au moment où il quitte un réseau ou y entre. Le trafic détourné peut alors être filtrer, l'empêchant alors d'aller jusqu'à destination. Des efforts continus sont réalisés pour élaborer des outils encore plus efficaces, comme la Validation de l'origine de la route (ROV),[19] et renforcer les outils existants, comme la définition approfondie d'un « chemin plausible » dans l'acheminement arrière en monodiffusion (uRPF).[20]

Le **commun accord pour la sécurité de routage (MANRS)[21]** est un ensemble de pratiques visibles de référence pour que les opérateurs de réseau améliorent la sécurité du système de routage mondial. En 2014, un groupe d'opérateurs de réseau partageant la même vision ont élaboré le MANRS par une initiative volontaire. Il définit quatre actions simples mais concrètes à mettre en œuvre par les opérateurs de réseau pour améliorer énormément la sécurité et la fiabilité de l'Internet.[22] Les deux premières améliorations (le filtrage et la validation de l'origine de l'IP) résolvent les causes

11 Les réseaux *annoncent* aux autres les détails des adresses disponibles dans leur réseau ou les réseaux d'un client. Ces annonces permettent de déterminer la façon dont les routeurs décident d'acheminer le trafic jusqu'à sa destination. *les politiques d'annonces* déterminent ce qu'un réseau annoncera à son voisin.

12https://tools.ietf.org/html/rfc7908#section-2

13 Par exemple, un opérateur de réseau avec plusieurs fournisseurs en amont annonce à un fournisseur en amont qu'il a un chemin vers la destination grâce à un autre fournisseur en amont (souvent à cause d'une mauvaise configuration accidentelle). Ou un réseau important pourrait involontairement annoncer des routes à tous ses réseaux en aval. Si elle est malveillante, une fuite de route peut être utilisée pour une inspection et la reconnaissance du trafic, ou (souvent dans un cas accidentel) peut causer des tensions sérieuses à l'infrastructure.

14 Dans le cas d'une usurpation d'adresse IP, quelqu'un crée des paquets IP avec une fausse adresse IP d'origine pour cacher l'identité de l'expéditeur ou usurper l'identité d'un autre système. L'usurpation d'adresse IP peut être utilisée pour faire des attaques d'amplification du serveur de nom de domaine (DNS)

15 Une attaque d'amplification du DNS est réalisée en envoyant de nombreuses requêtes à de nombreux résolveurs DNS en usurpant l'adresse IP de la victime ; un attaquant peut demander de nombreuses réponses des résolveurs DNS pour répondre à une cible, tout en n'utilisant qu'un système unique pour réaliser l'attaque.

16 https://www.us-cert.gov/ncas/alerts/TA14-017A

17 Chaque réseau détermine ce qu'il acceptera comme annonce des autres réseaux, c'est sa *« politique de filtrage ».*

18 La validation de l'origine de l'IP est une des techniques utilisées que l'adresse IP donnée par un paquet provient d'une adresse source valide.

19 https://www.nccoe.nist.gov/sites/default/files/library/sp1800/sidr-piir-nist-sp1800-14-draft.pdf

20 https://tools.ietf.org/html/draft-sriram-opsec-urpf-improvements-03

21 https://www.manrs.org/

22 https://www.manrs.org/manrs/

fondamentales des incidents de routage courants. Les deux autres, (coordination[23] et validation mondiale[24]) contribuent à limiter l'impact des incidents et diminuent la probabilité d'incidents à l'avenir.

Chaque action du MANRS prescrit les résultats plutôt que des méthodes spécifiques. Ceci permet la mise en œuvre du changement dans la technologie. Le MANRS cherche, en dehors des incidents de routage, à résoudre les défis de l'écosystème dans le système de routage mondial. Le MANRS améliore les incitations économiques à la sécurisation du routage en permettant aux opérateurs de réseau de signaler leur position sur la sécurisation du routage aux clients, concurrents et décideurs politiques. Il procure aussi des indicateurs pour mesurer la sécurisation du routage. Les indicateurs du MANRS peuvent aussi être utilisés comme une précieuse évaluation d'une tierce partie des pratiques de sécurisation d'un opérateur de réseau.[25]

Malgré l'existence de solutions aux incidents de routage courants, les défis de l'écosystème en limitent l'utilisation.

- **Les incidents de routage sont difficiles à résoudre à distance de l'origine et doivent donc être résolus collectivement.** Quelle que soit l'origine d'une menace, les réseaux les plus proches de l'origine sont les mieux positionnés pour résoudre la menace (p. ex. les réseaux adjacents peuvet refuser d'accepter les fausses annonces).[26] Quand un réseau éloigné de l'origine est impacté par un incident de routage, il ne peut qu'essayer d'en atténuer l'impact. Il doit s'appuyer sur les autres réseaux plus proches de l'origine de l'incident de routage pour résoudre complètement le problème.

- **Externalités économiques.** N'importe quel réseau peut être à l'origine d'un incident et l'absence de sécurité d'un réseau peut impacter l'ensemble des autres. Toutefois, même si un incident de routage se produit dans le propre réseau d'un opérateur, l'impact se fera très probablement sentir dans les autres réseaux. Les opérateurs de réseau sont peu enclins à dépenser des ressources sur une sécurisation du routage dans la mesure où ce sont plutôt les autres qui en récolteront les bénéfices, et non pas eux.

- **La sécurisation du routage n'est pas un différenciateur de marché.** Une bonne sécurisation du routage n'est pas actuellement un instrument de marketing pour les opérateurs de réseau. Les opérateurs de réseau trouvent difficile de communiquer leur niveau de sécurisation de routage à leurs clients. Les utilisateurs n'ont qu'une compréhension limitée du système de routage mondial et de l'impact sur eux des pratiques de sécurisation du routage de leur réseau.

23 Puisque les incidents de routage sont résolus plus facilement lorsqu'ils sont proches de leur origine, les actions d'amélioration de la coordination entre les opérateurs de réseau (qui peut être aussi simple que d'avoir ses coordonnées publiquement disponibles et mises à jour) sont vitales.

24 En documentant publiquement leur politique de routage et ce qu'ils pensent annoncer aux parties externes, les autres peuvent valider leurs annonces.

25 Un portail en ligne pour connaître ces indicateurs, l'observatoire MANRS, est en cours d'élaboration et devrait être disponible fin 2018.

26 « En politique, une telle approche est appelé un principe subsidiaire : les solutions peuvent être définies et mises en œuvre par l'autorité compétente la plus petite, la plus basse ou la moins centralisée. »
https://www.internetsociety.org/collaborativesecurity/approach/#_ftnref5

Recommandations et principes directeurs

L'action collective mondiale est la seule façon de résoudre les menaces à la sécurisation du routage et de renforcer cette même sécurisation. Toutes les parties prenantes, y compris les gouvernements, ont un rôle important à jouer pour améliorer les incitations du marché pour une meilleure sécurisation du routage, conduire l'élaboration ou l'adoption de meilleures pratiques, faire disparaître les barrières et renforcer la coopération. Toutefois, toute action doit être réalisée avec attention pour ne pas limiter les forces du système de routage mondial, y compris sa résilience globale, sa facilité d'utilisation, sa souplesse et son extensibilité. Pour améliorer la sécurisation du routage, nous devrions :

- **prêcher par l'exemple.** Toutes **les parties prenantes, y compris les gouvernements doivent améliorer la sécurité et la fiabilité de l'infrastructure en adoptant les meilleures pratiques pour leurs propres réseaux.**
    - Tous les réseaux offrant une connectivité à Internet, y compris les réseaux d'entreprise ou gouvernementaux, devraient utiliser le filtrage avec la validation de l'origine de l'IP pour participer à la prévention et l'atténuation des incidents.
    - De plus, les acteurs de marchés influents, comme les grandes entreprises ou les gouvernements devraient, lorsque c'est possible, exiger de leurs fournisseurs de service Internet la conformité à la sécurisation du routage de référence, comme celle présentée par le MANRS pour leurs contrats d'approvisionnement. Le MANRS offre par l'intermédiaire de son observatoire les indicateurs qui peuvent servir de précieuses évaluations d'une tierce partie des pratiques de sécurisation d'un opérateur de réseau. Ces évaluations peuvent participer à la prise de décision d'approvisionnement informée.
- **faciliter et encourager l'adoption de pratiques communes de sécurisation du routage.** Les associations d'industries, en étroite collaboration avec les gouvernements et autres parties prenantes, devraient promouvoir des références communes de sécurisation du routage.
    - Offrir des références communes aux opérateurs de réseau permet d'avoir des normes par industrie pour la sécurisation du routage et promeut un plus grand partage des informations parmi les opérateurs de réseau. Cela fournit aussi aux opérateurs de réseau une méthode pour informer la clientèle potentielle de leur niveau de sécurité.
    - Toutes les parties prenantes peuvent contribuer à l'élaboration et l'adoption de références communes et des pratiques par industrie de sécurisation du routage en participant à l'élaboration des processus et si possible, à leur financement.
- **soutenir les efforts réalisés dans l'élaboration de nouveaux outils de sécurisation du routage ou le renforcement des outils existants.** Pour améliorer davantage la sécurité du système de routage mondial, les partenariats au sein de la communauté de chercheurs peuvent contribuer à l'élaboration de la nouvelle génération d'outils et de pratiques de sécurisation du routage.
    - Si possible, les parties prenantes, y compris les gouvernements et le secteur privé peuvent augmenter le financement pour la recherche, l'élaboration et le déploiement expérimental de la nouvelle génération de protocoles Internet, y compris ceux qui améliorent la sécurisation du routage.

- Les chercheurs peuvent élaborer des principes généraux sur la façon d'exécuter la validation de l'origine de l'IP, un filtrage efficace et une validation mondiale. Les conseils doivent aussi encourager les opérateurs de réseau à mettre en œuvre BGPSec[27] et RPKI.[28]

- **encourager l'utilisation de la sécurité comme différenciateur concurrentiel.** Pour utiliser la sécurisation du routage comme différenciateur concurrentiel, les parties prenantes doivent **encourager la sensibilisation du public à l'importance de la sécurisation du routage et encourager une amélioration de la communication à propos de la sécurisation du routage entre le secteur et ses clients.**

  - Pour les fournisseurs de service Internet, la sécurisation du routage est un composant clé de leur politique de sécurité globale. Informer sur leur attitude face à la sécurisation du routage illustre fortement leur politique globale et peut différencier leurs services de ceux de la concurrence.

  - Les entreprises paieront davantage une meilleure sécurisation du routage, toutefois, ils doivent avoir les moyens de différencier la bonne sécurisation du routage de la mauvaise. Dans le cadre d'une étude de 2017, 94 % des entreprises indiquent accepter de payer davantage un fournisseur membre du MANRS dans le cas d'une situation concurrentielle.[29] La même étude a aussi déterminé que la sensibilisation au MANRS était marginale dans les entreprises avant cette dernière.

  - L'industrie, les groupes de clients, les gouvernements et les autres parties prenantes doivent travailler ensemble à la promotion de l'utilisation des sécurisations du routage de référence, tels que MANRS comme différenciateurs concurrentiels. [30] De plus elles doivent soutenir les efforts de formation auprès des entreprises locales au sujet de la sécurisation du routage et des meilleures pratiques existantes.

- **renforcer la communication et la coopération entre les opérateurs de réseau et les autres parties prenantes.** Les parties prenantes doivent soutenir l'élaboration de meilleurs mécanismes de partage des informations, participer à l'échange d'informations sur la sécurisation du routage et collaborer avec les autres parties prenantes à la résolution des menaces de sécurisation du routage.

  - Le secteur privé, les gouvernements, la société civile, les universités et les autres peuvent soutenir la mise en place ou le renforcement des équipes de réponse aux incidents de sécurité informatique (CSIRT). Les CSIRT jouent un rôle important dans les échanges d'informations et la coordination pour répondre aux incidents de routage et aux menaces liées.

---

27 BSGSec est une extension du Border Gateway Protocol (BGP) qui offre une sécurité pour le chemin des systèmes autonomes (AS) par lesquels un message de mise à jour BGP passe. https://tools.ietf.org/html/rfc8205

28 « Avec RPKI, l'infrastructure à clé publique de ressource, les annonces d'acheminement Border Gateway Protocol qui sont émises par un routeur sont validées pour garantir que la route provient du détenteur de la ressource et que c'est une route valide ». https://www.arin.net/resources/rpki/

29 Rapport d'étude sur le projet MANRS. 451 informations de recherche. https://www.routingmanifesto.org/wp-content/uploads/sites/14/2017/10/MANRS-451-Study-Report.pdf

30 Le MANRS en tant qu'ensemble visible de meilleures pratiques et par ses indicateurs publics fournis par l'observatoire MANRS, a le potentiel d'être un outil de marketing puissant pour les fournisseurs de service Internet.

- **identifie et répond aux obstacles juridiques posés par le partage d'informations, la mise en œuvre des technologies de sécurisation du routage et participent à la recherche à propos des incidents de routage et des menaces liées.** Des obstacles juridiques peuvent gêner les chercheurs et dissuader les opérateurs de réseau de déployer les solutions de sécurisation du routage et de partager les informations entre tous.

    - Identifier et éliminer les obstacles juridiques et réglementaires peuvent améliorer le partage d'informations et les réponses aux incidents de routage. Les parties prenantes, en particulier les chercheurs en sécurité peuvent craindre que la divulgation d'incidents de sécurisations du routage et les menaces liées les placent en mauvaise position juridique. Les obstacles juridiques peuvent aussi ralentir l'élaboration et le déploiement de technologies de sécurisation du routage. En élaborant des solutions pour identifier les obstacles, les parties prenantes doivent faire très attention à leurs impacts potentiels sur la protection de la vie privée des personnes.

Conclusion

Le système de routage mondial est incroyablement résilient. Sa structure décentralisée offre souplesse, extensibilité et longévité. Bien que sa structure ait joué un rôle crucial dans la croissance de l'Internet, elle a aussi permis aux incidents de se produire.

Les meilleures pratiques comme le commun accord pour la sécurité de routage fournissent aux opérateurs de réseau une direction claire pour résoudre ces menaces de routage. Toutefois, toutes les parties prenantes doivent prendre des mesures pour relever les défis de l'écosystème faisant obstacle à une large application des meilleures pratiques. Seule l'action collective nous permettra de relever les défis de la sécurisation du routage tout en conservant les avantages d'un système de routage décentralisé.