RFC 7855 : Source Packet Routing in Networking (SPRING) Problem Statement and Requirements

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 22 juin 2016

Date de publication du RFC : Mai 2016

https://www.bortzmeyer.org/7855.html

Traditionnellement, la transmission d'un paquet IP au routeur suivant était faite uniquement sur la base de l'adresse de **destination**, sans tenir compte du reste du paquet. Et la décision est prise par chaque routeur, sur le trajet, en complète indépendance. Or, l'émetteur d'un paquet voudrait souvent décider de la route suivie ou, au minimum, l'influencer. C'est pour cela qu'il existe des mécanismes de **routage par la source** ("*source routing*"). Leurs défauts et leurs limites ont mené à la recherche d'une meilleure solution, dite SPRING ("*Source Packet Routing In NetworkinG*"). Ce RFC est la description du problème.

Notez que le terme « source » a, pour SPRING, un sens plus large que lorsqu'on parle habituellement de "*source routing*". Dans ce dernier cas, la source était uniquement l'émetteur original. Pour SPRING, la source est l'endroit où on définit la politique de routage ultérieur, elle peut se situer au milieu du trajet.

Avant SPRING, il y avait plusieurs solutions permettant à la source de décider du routage mais aucune n'a été largement déployée (à part MPLS). C'est dû en partie à leur manque de souplesse, en partie à des problèmes de sécurité.

La future solution SPRING doit être un meilleur système (section 1 du RFC), et déployable de manière incréméntale (il ne serait évidemment pas réaliste de devoir changer tout l'Internet). En outre, l'état doit être maintenu dans le paquet lui-même, pas dans les routeurs intermédiaires. L'expérience de l'Internet a en effet largement montré que pour faire marcher un grand réseau complexe, il ne faut pas maintenir d'état dans les nœuds intermédiaires.

SPRING devra être assez général marcher avec plusieurs mécanismes de transmission des paquets ("*dataplanes*", cf. section 2). Les principaux visés sont MPLS et IPv6 avec un nouvel en-tête de routage (cf. RFC 2460 [1], section 4.4).

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc2460.txt

La section 3 présente plusieurs scénarios d'usage, pour montrer pourquoi un système tel que SPRING est utile. Il y a par exemple la création de tunnels pour faire des VPN (RFC 4364).

Il y a aussi le reroutage rapide de paquets (FRR, "*Fast ReRoute*"), et bien sûr l'ingéniérie de trafic. Pour ce dernier scénario, notre RFC demande que la future solution SPRING permette des options strictes (le paquet suit exactement le chemin spécifié) ou laxistes (le paquet suit à peu près le chemin spécifié), puisse fonctionner en centralisé (SDN) ou en décentralisé, etc.

Une des raisons du peu de déploiement des solutions de routage par la source est évidemment la sécurité (section 4 du RFC). SPRING met le chemin désiré dans le paquet (pour éviter de garder un état dans le réseau). Or, si on suit aveuglément les desiderata de chaque paquet, on ouvre la voie à des tas d'attaques. Par exemple, un paquet spécifie un détour considérable par un autre pays, et cela occupe pour rien les liaisons internationales. Un paquet spécifie un trajet qui boucle et les routeurs qui lui obéiraient feraient une attaque par déni de service contre eux-mêmes.

Le RFC impose donc que SPRING fournisse un mécanisme de « domaines de confiance » avec des frontières bien claires. Si un paquet vient d'un domaine de confiance, on lui obéit. S'il vient de n'importe où sur l'Internet, on ignore ses demandes (ou bien on vire ces options de routage par la source lorsque le paquet change de domaine).

La réalisation concrète de SPRING sur un système de transmission donné (comme MPLS ou IPv6) doit également documenter les risques spécifiques à ce "*dataplane*". Par exemple, MPLS est en général utilisé uniquement à l'intérieur d'un domaine contrôlé et connu (le réseau d'un opérateur) alors qu'IPv6 est de bout en bout donc pose davantage de risques (mais il dispose de possibilités supplémentaires, comme la signature cryptographique des en-têtes).

Il faut maintenant attendre les RFC décrivant les solutions, ils sont en cours de développement dans le groupe SPRING <https://tools.ietf.org/wg/spring/>.