RFC 5210 : A Source Address Validation Architecture (SAVA) Testbed and Deployment Experience

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 26 juin 2008

Date de publication du RFC : Juin 2008

https://www.bortzmeyer.org/5210.html

On le sait, l'Internet ne dispose pas de moyen de garantir l'authenticité de l'adresse IP de l'expéditeur d'un paquet. Le projet SAVA ("*Source Address VAlidation*", il ne semble pas avoir de page Web mais il existe une liste de diffusion <http://mail.nrc.tsinghua.edu.cn/cgi-bin/mailman/listinfo/sava>) vise à explorer les moyens de valider les adresses IP source. Il est actuellement à un stade très préliminaire mais une première expérience en vraie grandeur a été tentée en Chine et ce RFC la documente.

Si l'Internet n'authentifie pas les adresses IP, ce n'est pas, comme on le lit souvent, parce que ses concepteurs étaient naïfs, trop confiants dans la nature humaine, ou bien parce qu'ils étaient distraits et avaient oublié cette fonction. C'est parce que le problème est très difficile dans un réseau ouvert comme l'Internet. Si les réseaux X.25 vérifiaient les numéros des appelants, c'est simplement parce qu'il n'existait qu'un petit groupe d'opérateurs (seulement deux aux États-Unis et un seul en France) et que leurs clients devaient passer par un opérateur (pas de connexion directe). C'est aussi parce que ce petit groupe fermé d'opérateurs était uniquement situés dans les pays de l'OCDE. Dans l'Internet d'aujourd'hui, si une université thaïlandaise vérifie les adresses IP des machines de ses étudiants, par quelque moyen que ce soit, pourquoi un site gouvernemental brésilien, situé à plusieurs AS de là en tiendrait-il compte ?

(Il faut également mentionner les cas où il n'est même pas évident de savoir qui est le titulaire légitime d'une adresse, comme ce fut le cas lors du récent problème avec le serveur racine L <https://www.bortzmeyer.org/qui-controle-les-serveurs-racine.html>.)

Plusieurs tentatives d'authentifier les adresses IP ont déjà eu lieu. Les documents les plus souvent cités sur ce travail sont les RFC 2827[1] et RFC 3704. Si tous les opérateurs appliquaient ces RFC et

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc2827.txt

qu'on pouvait avoir confiance en tout le monde, le problème de l'usurpation d'adresses IP disparaitrait. Comme ce n'est pas le cas, le projet SAVA aborde le problème différemment.

SAVA est à la fois plus ambitieux (puisqu'il vise à permettre l'authentification de toute adresse IP partout dans le monde) et plus modeste, puisqu'il est bâti sur le prémisse que tout le monde n'adoptera pas SAVA (en tout cas, pas imémdiatement), et que peu d'opérateurs en déploieront immédiatement toutes les composantes et qu'il faut donc qu'il y aie des bénéfices même pour les premiers adoptants (ce qui manque au RFC 2827).

Le principe de SAVA est que chacun vérifie ce qu'il peut (il n'y a pas obligation de vérifier chaque adresse IP, une vérification du préfixe est déjà appréciable) et qu'il le communique à ceux qui le veulent. Selon les relations de confiance entre opérateurs, ces informations se propageront plus ou moins loin.

Le réseau chinois de la recherche et de l'enseignement CRNET a décidé de monter un test en grandeur nature de SAVA, dans son état actuel (SAVA n'est pas du tout normalisé, pour des raisons à la fois techniques et politiques.) Ce RFC est le compte-rendu de cette expérience. Douze sites ont participé à l'expérience, qui n'était donc pas une simple petite manipulation de laboratoire.

La section 2 du RFC résume les principes de SAVA, notamment le caractère « multi-barrières » (les vérifications peuvent se faire à divers endroits, puisqu'il n'est pas réaliste de les imposer, on aura donc toujours des cas où l'autre n'aura pas validé les adresses). Autre règle de SAVA : le fait que plusieurs mécanismes de vérification peuvent coexister. Non seulement il ne serait pas réaliste techniquement d'utiliser le même mécanisme pour un réseau Wifi et pour un réseau national, mais cette souplesse dans le choix des techniques de validation permet de maximiser le nombre de participants. SAVA se veut donc plus réaliste que les incantations habituelles « Il faudrait que tout le monde mette en œuvre le RFC 2827 ». Actuellement, dans SAVA, les vérifications peuvent se faire dans le réseau local, à l'intérieur de l'AS (c'est la seule possibilité dans le RFC 2827) ou bien entre AS. Autant que possible, SAVA réutilise des techniques existantes.

Les sections suivantes du RFC détaillent ces trois possibilités. La 2.2 explore les moyens de vérifier les adresses IP sur le réseau local, par exemple en ayant un commutateur qui interagisse avec le protocole d'allocation d'adresses IP. Aujourd'hui, le commutateur Ethernet est typiquement ignorant des allocations faites, par exemple avec DHCP et ne peut donc pas vérifier les adresses. Si ce commutateur jouait un rôle dans DHCP, il connaitrait les adresses IP qui peuvent apparaitre sur chaque port physique et pourrait les valider (cette technique se répand depuis : RFC 7513).

La section 2.3 traite la validation à l'intérieur de l'AS en recommandant simplement l'usage des techniques du RFC 2827 et RFC 3704.

Et les sections 2.4 et 2.5 traitent de la validation des adresses IP entre deux AS. 2.4 s'occupe du cas où les deux AS sont directement connectés. Dans ce cas, le problème est bien connu, chaque AS doit n'accepter de son voisin qu'un jeu limité de préfixes, enregistré dans un registre comme les IRR. Notons que l'expérience du détournement de YouTube par Pakistan Telecom <https://www.bortzmeyer.org/pakistan-pirate-youtube.html> a bien montré que cette pratique restait minoritaire, en partie parce que les IRR sont de qualité médiocre et en partie parce qu'elle impose un travail supplémentaire à tous. Certes, cette affaire portait sur le non-filtrage des annonces BGP et pas sur le non-filtrage des adresses IP mais rien ne permet de penser que le second filtrage sera fait plus sérieusement que le premier.

Plus délicat techniquement est le cas où les deux AS ne sont pas connectés directement. La solution préconisée par SAVA (sections 2.5 et 5.3) est alors l'utilisation d'un en-tête IPv6 spécial (l'expérience a

été faite dans un environnement purement v6, ces en-têtes sont décrits dans le RFC 2460, section 4.3), le "*authentication tag*". Signé cryptographiquement, cet en-tête permet de s'assurer que les routeurs des AS intermédiaires n'ont pas « bricolé » les adresses.

Après ces principes, la section 3 décrit l'expérience effective. La Chine a changé depuis « Tintin et le lotus bleu ». Le réseau CNG1-CERNET2 <http://www.chinadaily.com.cn/english/doc/2004-12/27/content_403512.htm>, utilisé pour le test, connecte vingt-cinq sites, répartis dans tout le pays, à des débits allant jusqu'à 10 Gb/s. Il comprend plusieurs AS et est purement IPv6. L'expérience n'a utilisé qu'une moitié de ces sites, mais a mis en œuvre les trois scénarios de validation décrits en section 2. Les douze sites participants n'ont pas tous déployé ces trois scénarios, ce qui permet de tester SAVA dans le cas (réaliste) où tout le monde n'est pas au même niveau de déploiement.

La section 4 présente les résultats de l'expérience et proclame qu'elle fut un succès. Les paquets usurpateurs injectés dans le réseau, ont été tous jetés tôt ou tard. Les performances n'ont pas toujours été au rendez-vous, par exemple le routeur IPv6 routait toutes les extensions "*hop-by-hop*" en logiciel, donc à des performances catastrophiques pour des liaisons si rapides.

Cela ne veut pas dire que SAVA, tel que déployé dans le banc de test, soit parfait. La section 5 détaille ses limites et devrait être lue par tous ceux qui s'indignent bruyamment que l'Internet ne leur offre pas encore le niveau de traçabilité qu'ils réclament. D'abord, il faut noter qu'il y a belle lurette que la majorité des attaques sur Internet ne sont plus effectuées en trichant sur l'adresse IP. Les zombies ne se soucient en effet pas de déguiser leur adresse. D'autre part, même si SAVA peut commencer localement, une validation de bout en bout nécessitera en général la coordination de plusieurs AS, chose très difficile à obtenir. Enfin, la section 5 note que des techniques comme le "*multihoming*" ou la mobilité compliquent encore les choses.

Reste à savoir ce que deviendra SAVA. La section 6 propose une synthèse en affirmant que l'expérience a été un succès mais que le protocole doit être considérablement amélioré. Le cadre général et les protocoles ne sont pas encore normalisés et l'IETF n'a pas encore accepté un groupe de travail pour le faire (un groupe de travail avec une charte plus restreinte, SAVI, a été proposé mais pas encore accepté), SAVA soulevant bien des problèmes, notamment politiques. Ce n'est pas par hasard que la première expérimentation de SAVA sur le terrain aie eu lieu dans un pays gouverné par une dictature. Dans les couloirs de l'IETF, on entend souvent des protestations contre une technique qui rendrait la tâche des policiers chinois plus facile.