RFC 6959 : SAVI Threat Scope

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 30 mai 2013

Date de publication du RFC : Mai 2013

https://www.bortzmeyer.org/6959.html

On sait que, sur l'Internet, il est possible et même facile d'usurper une adresse IP , c'est-à-dire d'émettre un paquet IP avec une adresse source allouée à quelq'un d'autre (ou pas allouée du tout). Le projet SAVI ("*Source Address Validation Improvement*") vise à améliorer la validation de l'adresse source, de manière à rendre l'usurpation plus rare et plus difficile. Ce RFC décrit la menace à laquelle SAVI répondra et étudie les contre-mesures existantes.

L'Internet emploie un protocole de réseau sans connexion (que ce soit en IPv4 ou en IPv6). Lorsqu'une machine veut communiquer avec une autre, elle met son adresse IP comme source d'un paquet, celle de son correspondant en destination et elle envoie le paquet. Substituer l'adresse IP d'une autre machine à la sienne est donc aussi simple que d'écrire une autre chaîne de bits à la place de l'adresse authentique. Le réseau n'essaie pas d'empêcher cela. Certes, le fraudeur ne pourra pas forcément recevoir les réponses (elles arriveront à celui dont l'adresse a été usurpée) mais ce n'est pas forcément un problème dans un réseau sans connexion. Il existe des mécanismes pour empêcher cette usurpation, le plus connu étant BCP 38 <https://www.bortzmeyer.org/bcp38.html> (les RFC 2827[1] et RFC 3704) mais ils sont insuffisamment déployés, car ils n'apportent pas de bénéfices à celui qui les déploie, uniquement aux autres acteurs de l'Internet. En outre, BCP 38 ne protège pas toujours suffisamment. Par exemple, s'il est mis en œuvre dans le premier routeur, il n'empêchera pas les machines du LAN d'usurper les adresses de leurs voisines.

L'une des idées de SAVI est donc de compléter BCP 38 avec des validations locales, apportant un bénéfice local, et qui permettraient une meilleure traçabilité.

Quelques termes à apprendre pour bien suivre les documents sur SAVI :

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

— "*Bind anchor*" : l'information sur laquelle on se base pour valider une adresse IP source. Par exemple, sur un commutateur, cela pourra être l'adresse MAC ou bien le port physique du commutateur.
— Routeur NNI ("*Network to Network Interface*") : un routeur qui fait face à un routeur d'un autre opérateur.
— Routeur PE ("*Provider Edge*") : un routeur qui fait face au client d'un opérateur.
— RPF ("*Reverse Path Forwarding*") : valider une adresse source en regardant si la réponse au paquet entrant partirait ou non par l'interface sur laquelle il est entré (détails dans le RFC 3704).

La section 3 détaille ensuite les attaques rendues possibles, ou facilitées par l'usurpation d'adresses IP source (la section 4 couvrira les contre-mesures). D'abord, les attaques en aveugle : l'assaillant, qui a usurpé l'adresse IP source, ne peut pas recevoir les réponses à ses paquets. Il peut les envoyer, ces paquets, mais c'est tout. Cela lui complique évidemment sérieusement la vie. Certaines attaques restent possibles. Il y a celles ne nécessitant qu'un seul paquet (et donc pas de réponse). Par exemple, si un paquet spécialement construit plante le logiciel du routeur qui le traite, un attaquant peut monter une attaque par déni de service en envoyant un unique "*packet of death*". Un autre cas est celui où, en envoyant un paquet où l'adresse source et destination sont identiques, le destinataire se réponde à lui-même, puis à la réponse de la réponse, et entretienne ainsi lui-même la boucle sans fin (une bogue de cette famille avait frappé PowerDNS <http://doc.powerdns.com/html/powerdns-advisory-2012-01.html>).

Une autre attaque en aveugle est le RST ("*ReSeT*") TCP usurpé (section 2.3 du RFC 4953). Un seul paquet TCP accepté (l'attaquant doit deviner un numéro de séquence contenu dans la fenêtre en cours) va couper la connexion (notez que les protocoles applicatifs comme TLS et SSH ne sont d'aucune utilité contre cette attaque). Cela peut être très gênant pour les connexions censées durer longtemps (sessions BGP par exemple). Il existe des contre-mesures (voir le RFC 5961) mais empêcher l'usurpation d'adresse IP empêcherait complètement cette attaque.

Après les attaques en aveugle formées d'un seul paquet, place aux attaques volumétriques, reposant sur l'envoi d'un grand nombre de paquets. L'idée est de remplir certaines tables de taille fixe (par exemple la table des connexions entrantes) ou, encore plus simplement, de saturer le réseau de la victime. L'attaquant n'ayant pas besoin de réponse, il a tout intérêt, dans ces paquets, à usurper l'adresse IP source pour déguiser son identité. On constate que beaucoup de gens n'ont pas encore compris la facilité avec laquelle cette usurpation est possible, et croient réellement que l'adresse IP source qu'ils observent dans les paquets entrants est réellement celle de leur attaquant (pensez à cela la prochaine fois que vous lirez dans les médias quelque chose du genre « attaque par déni de service contre tel organisme, l'examen de l'attaque montrait que l'attaquant venait de Russie/Chine/Moyen-Orient »). Pire, la victime bloque parfois les paquets IP entrants en fonction de cette adresse source, réalisant ainsi une autre attaque par déni de service, contre la victime de l'usurpation d'adresse. Certaines attaques peuvent d'ailleurs être montées dans ce seul but.

Une autre raison pour l'attaquant d'usurper l'adresse IP source est la possibilité d'**attaque par réflexion** : comme au billard, on va viser une autre boule que celle qu'on veut vraiment toucher. L'attaquant envoie un paquet UDP au réflecteur (qui n'est pas sa vraie victime, juste un complice involontaire) en usurpant l'adresse IP source de la victime. Le réflecteur va alors répondre à ce qu'il croit être l'émetteur et qui est en fait la victime, qui sera ainsi bombardée par le ou les réflecteurs. La réflexion sert à l'attaquant à dissimuler ses traces (le paquet va suivre un tout autre chemin dans le réseau) mais elle est surtout intéressante couplée avec l'**amplification**. Avec certains protocoles, la réponse va être plus grande, voire beaucoup plus grande, que la requête. Avec une amplification de 20, l'attaquant pourra ainsi obtenir un bombardement de 1 Gb/s en ne dépensant lui-même que 50 Mb/s. Plusieurs protocoles permettent l'amplification, comme NTP, SNMP et surtout le DNS comme ce fut le cas lors de l'attaque de 2006 <http://www.verisign.com/static/037903.pdf> (le RFC ne les cite pas mais des attaques plus violentes ont eu lieu en 2012 et 2013).

Le RFC classe aussi dans les attaques volumétriques les actions visant à empoisonner les données d'un serveur distant. Le cas le plus courant est celui des empoisonnements DNS où le méchant va tenter de répondre avant le serveur légitime (cas, par exemple, des attaques Kaminsky <https://www.

bortzmeyer.org/comment-fonctionne-la-faille-kaminsky.html>). Ici, le volume élevé des requêtes n'est pas dû au désir de saturer la victime, mais à la nécessité de faire beaucoup d'essais pour en voir un accepté. (Dans le cas du DNS, il s'agit d'essayer beaucoup de "*Query ID*" et de ports source UDP.) À noter qu'il existe aussi des attaques par empoisonnement contre les caches ARP.

Cela, c'était les attaques en aveugle. Mais, parfois, un attaquant qui usurpe une adresse IP peut observer les réponses, par exemple parce qu'il est sur le même réseau local à diffusion que la victime de l'usurpation ou bien, si le réseau local ne diffuse pas à tous, parce qu'il a empoisonné les caches ARP. L'attaquant a alors bien plus de possibilités comme le détournement d'une connexion TCP à son profit, les tests de vulnérabilité d'un objectif sans se trahir, la subversion des protocoles de routage en se faisant passer pour un des routeurs participants, etc.

La section 4 décrit ensuite les contre-mesures qui peuvent être adoptées aujourd'hui et qui sont effectivement déployées, au moins partiellement. Par exemple, un commutateur peut (en violant légèrement le modèle en couches), refuser les paquets dont l'adresse IP source ne correspond pas à l'adresse MAC du paquet (que le commutateur a pu apprendre en examinant les requêtes et réponses ARP). Ou bien ceux qui viennent d'un autre port physique que d'habitude. Si les paquets de `192.168.7.64` venaient toujours du port 3 et que, tout à coup, ils viennent du port 4, le commutateur peut soupçonner une usurpation (ou tout simplement une machine qui a été déplacée : la sécurité peut se tromper).

On peut donc jeter un paquet lorsque son adresse IP source ne correspond pas aux informations qu'on possède. Notez bien que, plus on s'éloigne de la source des paquets, plus il est difficile d'être sûr que c'est bien une usurpation. Néanmoins, le RFC identifie cinq endroits où peut se faire cet examen de validité, du plus proche de la source au plus éloigné :

— Sur le lien où est attachée la machine, comme dans l'exemple du commutateur ci-dessus. On dispose au moins de l'adresse MAC, ce qui facilite le test. Si le médium est complètement partagé (lien Wi-Fi, Ethernet classique...), cela s'arrête là. Mais, dans la cas contraire, on a aussi souvent une information physique, comme le port du commutateur. C'est donc clairement le meilleur endroit pour valider et c'est là que porteront l'essentiel des efforts du projet SAVI (voir par exemple un des premiers RFC, le RFC 6620). Le RFC traite aussi les cas spécifiques des accès Internet par câble (technologie DOCSIS) ou par ADSL. Pour ce dernier, le premier équipement du FAI dans le réseau a en général largement assez d'informations pour empêcher qu'un abonné n'usurpe l'adresse d'un autre (mais pas pour empêcher qu'une machine chez un abonné n'usurpe l'adresse d'une autre chez le même abonné ; il n'est pas évident que ce soit un problème sérieux en pratique puisque c'est le même foyer).
— Les commutateurs suivants, auxquels la machine n'est pas directement connectée, peuvent aussi valider, mais de manière moins fiable. Si le "*spanning tree*" ou un autre protocole comme VRRP change la topologie, les paquets émis par une adresse IP donnée apparaîtront, et légitimement, sur un autre port. Les commutateurs pourraient donc avoir besoin de se transmettre leur état SAVI (liste des adresses valides et leurs ports, autrement dit les "*bind anchors*").
— Les routeurs peuvent ensuite être utilisés. À part le premier, ils n'ont pas l'adresse MAC à leur disposition. Le principal test qu'ils peuvent faire est de s'assurer que l'adresse IP source est dans un préfixe qui existe sur ce réseau. Par exemple, un routeur qui sait qu'il connecte `2001:db8:32:a17::/64` à l'Internet peut raisonnablement jeter un paquet venant du réseau local et prétendant avoir comme source `2001:db8:cafe::666`. Notez que le routeur ne peut en général rien faire contre une machine qui usurperait une adresse du même réseau local (ici, `2001:db8:32:a17::b00c` qui se ferait passer pour `2001:db8:32:a17::babe`). Dans des cas moins triviaux (routeurs avec beaucoup d'interfaces et ayant de nombreux préfixes derrière eux), pour savoir quels préfixes sont acceptables, le routeur peut simplement consulter une ACL maintenue manuellement ou alors utiliser RPF (RFC 3704).
— Un cas intéressant est le premier routeur du FAI, le routeur PE : le RFC 2827 demande explicitement que tous ces routeurs filtrent les paquets ayant une adresse IP qui n'est pas dans le préfixe alloué au client (voir aussi la section 4.2.1 de notre RFC). À noter qu'il ne peut pas aller plus loin et valider chaque adresse : cela nécessiterait que le client fasse ce filtrage (cf. les cas plus haut).

— Enfin, au niveau des routeurs NNI, on est très loin de la source et tout filtrage devient difficile. Qui plus est, on ne sait pas si l'opérateur en place filtre dans son propre réseau ou pas. L'ancien projet SAVA (précuseur de SAVI, mais beaucoup plus ambitieux) espérait monter une infrastructure de transmission d'informations sur la validation, permettant d'indiquer aux autres opérateurs l'étendue du filtrage qu'on avait fait sur son réseau. Le projet ayant été abandonné, il ne reste que les solutions non techniques comme de tenter de faire signer des engagements de validation d'adresse IP source à ses pairs BGP, en mettant ceux qui ne signent pas dans dans un « enfer » par exemple en étiquetant leurs annonces de préfixes avec une communauté BGP ad hoc (RFC 1997) et en la transmettant aux autres pairs (idée qui me semble personnellement très peu réaliste).

En pratique, il y a des tas de détails qui compliquent la validation d'adresse IP source. Par exemple, pour un commutateur réseau, le cas simple est celui où il y a une et une seule machine derrière chaque port physique et où chaque adresse MAC ne correspond qu'à une seule adresse IP. Si ce n'est pas le cas, le problème devient plus difficile. Pensez par exemple à une machine physique, connectée par le port d'un commutateur mais portant plusieurs machines virtuelles, chacune avec sa propre adresse IP et sans doute sa propre adresse MAC. Ce cas est en fait un commutateur interne, le commutateur physique n'étant que le deuxième commutateur sur le trajet et n'ayant donc que des capacités de validtaion limitées. Idéalement, c'est le commutateur virtuel dans le système de virtualisation qui devrait faire respecter les règles SAVI, mais l'administrateur réseaux n'en a pas forcément le contrôle et ne lui fait pas forcément confiance.

Pour apprendre le lien entre une adresse MAC et une adresse IPv4, la meilleure solution pour un commutateur est d'écouter les requêtes et les réponses DHCP et de considérer qu'elles font autorité au sujet de ce lien (cf. RFC 7513). Par exemple, en voyant passer cette réponse (vue avec tcpdump) :

```
09:49:23.191187 00:10:db:ff:40:70 > 18:03:73:66:e5:68, ethertype IPv4 (0x0800), length 368: (tos 0x0, ttl 64
    192.0.2.20.67 > 192.0.2.54.68: BOOTP/DHCP, Reply, length 326, hops 1, xid 0x903b4b00, Flags [none]
  Your-IP 192.0.2.54
  Client-Ethernet-Address 18:03:73:66:e5:68
          ...
```

Le commutateur sait alors que l'adresse IP `192.0.2.54` a été allouée à `18:03:73:66:e5:68` et qu'un paquet IP dont l'adresse MAC source serait `18:03:73:66:e5:68` et l'adresse IP source serait autre chose que `192.0.2.54` est probablement une usurpation et doit être jeté.

Pour IPv6, outre le trafic DHCP, le commutateur doit écouter les paquets DAD ("*Duplicate Address Detection*") du protocole d'auto-configuration (RFC 4862). Le commutateur sera alors au courant des adresses IP légitimement enregistrées, et de l'adresse MAC correspondante, et pourra se servir de cette information pour valider. Par contre, contrairement à ce qu'on pourrait penser, le protocole d'authentification 802.1x n'aide pas : il authentifie un utilisateur mais ne limite pas les adresses IP qu'il peut utiliser. Enfin, il existe des techniques cryptographiques qui pourraient être utiles pour SAVI comme le SEND du RFC 3971 mais qui sont tellement peu déployées qu'on ne peut pas réellement compter dessus.

Certaines topologies de réseau, quoique parfaitement légales, peuvent sérieusement handicaper SAVI (section 5). Par exemple, si toutes les adresses sont statiques et stables, le problème est relativement bien circonscrit. Mais dans beaucoup de réseaux, ce n'est pas le cas et des adresses sont attribuées dynamiquement. Une même adresse IP sera, dans le temps, allouée à plusieurs adresses MAC et une même adresse MAC n'aura pas forcément la même adresse IP à chaque visite de ce réseau. (Ceux qui utilisent arpwatch sur un tel réseau savent le nombre d'« alarmes » que cela génère. SAVI a exactement le même problème.) D'autre part, si certaines machines sont simples (une adresses MAC, une adresse IP), d'autres sont plus complexes pour le validateur. Un exemple typique est un routeur. Par définition, il émet sur le réseau local des paquets avec sa propre adresse MAC mais des adresses IP source qui ne sont pas la sienne. Il est donc difficile de valider ces paquets.

Autre cas rigolo, notamment en cas de virtualisation : si une machine se déplace dans le "*data center*" mais garde son adresse IP. Les commutateurs vont devoir oublier la vieille information sur le port où est connecté cette machine et apprendre la nouvelle. (On appelle cela « mettre à jour son état SAVI ».)

La mobilité entraîne aussi des problèmes. Dans IP, elle peut se réaliser de plusieurs façons. Dans l'une, dite « en jambe de chien », la machine mobile émet des paquets avec son adresse IP source stable ("*home address*"), quel que soit le réseau physique où elle est attachée. Un tel mécanisme est évidemment incompatible avec toute solution de validation. Il faut donc que tous les paquets du mobile, aussi bien en émission qu'en réception, soient relayés par la station de base située sur son réseau d'attachement habituel.

Un petit mot aussi sur IPv6 : il crée des difficultés supplémentaires en raison de l'auto-configuration, très pratique mais, par son caractère local, non contrôlé centralement, pas forcément très sûre. Et son espace d'adressage très large (une bonne chose, et la principale raison pour laquelle il est important de déployer IPv6) a comme effet de bord la facilité à utiliser beaucoup d'adresses usurpées. En IPv4, un usurpateur a en théorie $2\hat{}32$ adresses à usurper et, en pratique, plutôt moins de $2\hat{}24$ (uniquement celles de son réseau local). En IPv6, même si on arrive à limiter l'usurpateur à son réseau local, il aura $2\hat{}64$ adresses, ce qui permet de court-circuiter certains mécanismes de sécurité.

La section 6 revient en détail sur la question de la **granularité** de la validation. Aujourd'hui, il est relativement facile d'empêcher les usurpations inter-sites (où un attaquant prend l'adresse IP d'une machine sur un autre site). Mais empêcher les usurpations intra-sites est plus complexe or, justement, la plupart des attaques viennent de l'intérieur.

Notez que SAVI se limite aux couches basses : il n'est pas prévu de vérifier les adresses IP qui apparaissent dans les applications (par exemple dans le champ `Received:` des messages formatés suivant le RFC 5322).

Enfin, la section 7 revient sur les questions de sécurité à un haut niveau. Elle rappelle que SAVI n'a pas pour but de produire des preuves, au sens judiciaire du terme (dans le meilleur cas, la validation permet de s'assurer de l'adresse IP, mais certaines machines sont multi-utilisateurs). Elle rappelle aussi que SAVI est une technique relativement légère et que, même si elle était massivement déployé, il ne faudrait pas utiliser les adresses IP source comme authentiques. La seule solution fiable pour être certain de l'identité de son correspondant est la cryptographie.

Cette section 7 revient aussi en détail sur les conséquences de SAVI pour la vie privée. Une adresse IP peut être vue, dans certains cas, comme une donnée identifiant une personne et le fait de la valider a donc des implications. Le RFC note bien que la validation SAVI ne nécessite **pas** d'enregistrer de l'information et que, si on réalise cet enregistrement avec des adresses IP, on peut engager sa responsabilité morale et/ou légale.

Aujourd'hui, des fonctions de type SAVI sont présentes dans pas mal de systèmes (par exemple les commutateurs haut de gamme) mais pas forcément toujours activées. Le RFC 5210 contient un compte-rendu d'expériences à ce sujet.