RFC 7513 : SAVI Solution for DHCP

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 11 juin 2015

Date de publication du RFC : Mai 2015

https://www.bortzmeyer.org/7513.html

Le cadre SAVI ("*Source Address Validation Improvement*"), décrit dans le RFC 7039 [1], vise à rendre plus difficile l'usurpation d'adresses IP. SAVI fournit un cadre général et plusieurs solutions techniques concrètes sont ensuite développées selon le type de réseau et selon le niveau de sécurité qu'on désire et qu'on est prêt à « payer ». Ainsi, le RFC 6620 décrivait un mécanisme où le réseau d'accès assurait que le premier titulaire d'une adresse IP puisse la garder. Ce nouveau RFC décrit un autre mécanisme, où c'est via l'utilisation de DHCP qu'on contrôle les adresses : le réseau d'accès va empêcher l'utilisation d'adresses qui n'ont pas été allouées par le serveur DHCP. (Ce mécanisme est largement déployé depuis des années, sous divers noms, comme « "*DHCP snooping*" », mais n'avait pas été formellement décrit dans un RFC.)

L'usurpation d'adresse IP est à la base de nombreuses attaques sur l'Internet, comme les attaques par réflexion <https://www.bortzmeyer.org/attaques-reflexion.html>. Il existe depuis longtemps des techniques pour limiter l'usurpation d'adresses IP (le RFC 2827 est un exemple classique, qui permet de protéger un réseau contre l'usurpation par un autre). Celles de SAVI visent surtout le réseau local (réseau d'accès pour un FAI) en limitant le risque d'usurpation interne (qu'un utilisateur du réseau local usurpe l'adresse d'un autre). Ici, dans ce RFC 7513, l'allocation d'une adresse IP via DHCP va créer un **lien** ("*binding*") entre cette adresse et des informations qui permettront au réseau de filtrer les usurpateurs. Par exemple, en retenant le port physique du commutateur comme lien, le commutateur peut bloquer les paquets dont l'adresse IP source n'est pas celle qui a été allouée à la machine connectée à ce port. Un tel mécanisme est souvent présent dans les commutateurs existants, souvent sous le nom de "*DHCP snooping*" mais attention : parfois, ce "*DHCP snooping*" se limite à bloquer les réponses DHCP arrivant sur un port inattendu, et n'intégre pas forcément la protection contre l'usurpation d'adresses IP, le but principal de ce RFC. Vérifiez avec votre commutateur !

Ce mécanisme de lien ("*binding anchor*") est décrit en section 3 du RFC 7039 et rappelé en section 3 de notre RFC. Un lien doit être un attribut caractéristique, et difficile à changer (un contre-exemple est

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc7039.txt

l'adresse MAC, facile à changer sur beaucoup de systèmes, et pourtant citée par notre RFC). C'est le cas du port physique du commutateur Ethernet cité plus haut, ou bien d'une association de sécurité WiFi (la section 3.2 du RFC 7039 donne d'autres exemples).

SAVI-DHCP va donc surveiller le trafic DHCP, notant les requêtes et réponses DHCP et les associant aux liens. Notez que cela marche avec le DHCP avec état (RFC 2131 pour IPv4 et RFC 8415 pour IPv6), pas avec le DHCP sans état du RFC 8415, qui ne s'occupe pas d'allocation d'adresses IP. De même, SAVI-DHCP ne gère évidemment pas le cas des réseaux où les adresses IP sont obtenues par un autre moyen que DHCP, par exemple le SLAAC du RFC 4862. Idem pour les adresses locales au lien (RFC 4291, section 2.5.6). Dans ces deux derniers cas, il faut utiliser une autre technique SAVI, le FCFS du RFC 6620.

Bon, maintenant, les détails. La section 4 précise quels acteurs sont considérés : un serveur DHCP évidemment, des clients DHCP, et les machines SAVI, typiquement des commutateurs, qui vont faire respecter les règles SAVI (il y a aussi quelques commutateurs non-SAVI dans le réseau d'exemple, pour mieux refléter la réalité). La machine SAVI va avoir besoin d'une certaine configuration. Par exemple, si le réseau contient un serveur DHCP menteur, la machine SAVI ne peut pas le deviner, et il faut lui dire sur quel port est attaché le vrai serveur DHCP (attribut SAVI `DHCP-trust`, cf. par exemple cette documentation Cisco <`http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/12-2SX/configuration/guide/book/snoodhcp.html#wp1114389`>, la commande `ip dhcp snooping trust` indiquera qu'un serveur DHCP légitime opère sur cette interface). De même, certains ports physiques ne doivent pas valider les adresses IP (attribut SAVI `Trust`, par exemple un port attaché au routeur de sortie, port sur lequel on verra passer, et c'est normal, plusieurs adresses IP) et il faudra donc indiquer à la machine SAVI sur quels ports elle doit surveiller (ceux où ne se trouve normalement qu'une ou plusieurs machines obtenant des adresses par DHCP).

SAVI sépare le réseau en deux, la partie de confiance et le reste. Dans la partie de confiance, on peut être raisonnablement sûr que les adresses IP source sont authentiques : tous les commutateurs valident. SAVI ne prétend pas sécuriser tout l'Internet. Et, même dans le réseau local, une partie du réseau peut être non-SAVI et ne sera donc pas de confiance. Cette notion de périmètre (séparant la partie de confiance et le reste) est essentielle pour configurer SAVI, et pour savoir ce qu'on peut attendre de cette technique. Par exemple, des réponses DHCP venues d'un serveur situé en dehors du périmètre ne seront pas utilisées par SAVI : puisque cette zone n'est pas de confiance, il peut parfaitement s'agir d'un serveur pirate (section 4.3.3 du RFC, un bon exemple de l'utilisation de la notion de périmètre, avec un schéma d'exemple).

La sécurité de SAVI-DHCP dépend évidemment de la sécurité des liens. Il faut notamment s'assurer que les attributs utilisés pour construire le lien sont difficiles à usurper. Un port physique du commutateur est un bon exemple. A contrario, une adresse MAC est un mauvais attribut (trop facile à changer) et même un attribut fort peut être affaibli par certains usages. Par exemple, si on utilise le port physique du commutateur Ethernet comme "*binding anchor*", mais que ce dernier est connecté à des commutateurs non-SAVI en cascade, les nombreuses machines qui partagent ce port physique peuvent encore usurper leurs adresses IP entre elles.

Ces liens et les adresses IP associées doivent être stockées dans la mémoire de la machine SAVI, dans un structure de données dite BST ("*Binding State Table*", section 5). Chaque ligne de cette table stocke également la durée de vie du lien et l'état du lien (établi, en cours d'établissement, inconnu).

La BST se remplit en « espionnant » ("*snooping*") le trafic DHCP (section 6). En résumant (beaucoup) : la machine SAVI voit passer une requête DHCP et la réponse arrive depuis un port marqué comme `DHCP-trust`. On stocke alors dans la BST le port d'où est venu la requête (le lien, le "*binding anchor*"), l'adresse IP dans la réponse, le fait que le lien est établi, et sa durée de vie (typiquement la durée du bail

DHCP). Désormais, si on voit un paquet IP arriver par le port d'où venait la requête DHCP, on pourra regarder son adresse IP source, et jeter le paquet si elle ne correspond pas à ce qui est dans la BST (ce filtrage est décrit en section 8). Sur un Juniper, on peut afficher cette BST avec `show dhcp snooping binding`. Cet exemple est tiré d'une documentation Juniper :

```
user@switch> show dhcp snooping binding
DHCP Snooping Information:
MAC Address             IP Address Lease   Type     VLAN    Interface
-----------------       ---------- -----   -------  ----    ---------
00:00:01:00:00:03       192.0.2.0  640     dynamic  guest    ge-0/0/12.0
00:00:01:00:00:04       192.0.2.1  720     dynamic  guest    ge-0/0/12.0
00:00:01:00:00:05       192.0.2.5  800     dynamic  guest    ge-0/0/13.0
```

Attention, il y a quelques pièges. Par exemple, s'il existe plusieurs chemins entre le client et le serveur DHCP, et que la machine SAVI n'est que sur un seul de ces chemins, elle risque de rater le dialogue DHCP. Autre cas problématique si une machine se déplace d'un port à un autre sans refaire une requête DHCP.

La section 7 propose des solutions à ces problèmes de faux positifs. L'idée est de noter le trafic rejeté par SAVI-DHCP et de vérifier activement si le paquet a été rejeté à tort (le mal nommé « "*Data Snooping Process*" »). Par exemple, en IPv4, on peut envoyer des requêtes ARP (RFC 826 et RFC 5227) pour déterminer si deux machines (la vraie et l'usurpatrice) utilisent la même adresse IP (s'il n'y a qu'une machine, la vraie, on ne recevra qu'une réponse). En IPv6, on peut utiliser un message DAD ("*Duplicate Address Detection*", cf. RFC 4862, section 5.4) pour faire le même test.

On peut aussi, si on a raté ou qu'on pense avoir raté le dialogue DHCP, demander directement au serveur DHCP, avec un message `DHCPLEASEQUERY` (RFC 4388) en IPv4 et `LEASEQUERY` (RFC 5007) en IPv6.

Bref, comme toujours en sécurité, on n'a pas de repas gratuit : SAVI-DHCP protège contre bien des usurpations mais, comme toute technique de filtrage, il peut mener au rejet de messages légitimes.

Le mécanisme de SAVI-DHCP nécessite de mémoriser un état, la BST ("*Binding State Table*", décrite en section 5). Si elle est gardée en RAM et qu'on redémarre, la liste des liens est perdue et tous les paquets seront rejetés (c'est pourquoi, en général, IP déconseille de garder de l'état dans le réseau). La section 9 rappelle ce problème et demande donc que la BST soit stockée dans une mémoire qui survit aux redémarrages. (On pourrait récupérer un bon bout de la BST par les méthodes de la section 7 mais ça prendrait un temps fou.) À noter que, sur un Juniper, ce n'est pas fait par défaut (il faut la directive `dhcp-snooping-file` pour stocker la BST).

Terminons ce résumé du RFC avec la section 11, consacrée aux questions de sécurité. D'abord, les risques que crée le "*Data Snooping process*" de la section 7. Comme ce processus est coûteux en nombre de paquets envoyés, un attaquant pourrait être tenté de le déclencher afin de réaliser une attaque par déni de service. Pour cela, il aurait juste à envoyer quelques paquets usurpés. Le processus doit donc avoir une limitation de trafic.

Plusieurs autres attaques sont possibles contre ce mécanisme de sécurité complexe qu'est SAVI-DHCP (réutiliser l'adresse d'un client qui est parti et ne peut donc plus se défendre en cas de détection d'adresse dupliquée, créer de nombreux liens pour remplir la BST et faire une attaque par déni de service, etc). Il y a aussi un risque sur la vie privée, puisque la BST stocke de nombreuses informations sur l'arrivée et le départ des machines des utilisateurs. Elle ne doit donc pas être archivée. L'idée est

qu'aucune information ne devrait être gardée sur les machines qui n'usurpent jamais d'adresse IP (ne pas fliquer les gens honnêtes).

À noter que Cisco prétend avoir inventé la technique et a un brevet <http://datatracker.ietf.org/ipr/2373/> sur l'idée, mais propose une licence (avec clause de représailles).

Merci à Cécile Grange pour des indications sur les solutions Juniper.