RFC 7039 : Source Address Validation Improvement Framework

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 1 novembre 2013

Date de publication du RFC : Octobre 2013

http://www.bortzmeyer.org/7039.html

Une des choses agaçantes sur l'Internet est qu'il est trivial de tricher sur son adresse IP source. Une machine qui a comme adresse 2001:db8:1:2::42 peut parfaitement émettre un paquet où l'adresse IP source est 2001:db8:9fe:43::1 et, là plupart du temps, ce paquet arrivera à destination (le routage ne se fait que sur la destination, pas sur la source), trompant le récepteur sur la vraie source de l'envoi. Cette faiblesse a donc des tas de conséquences pour la sécurité. Il existe des bonnes pratiques documentées pour empêcher l'émission de tels paquets (RFC 2827[1] et RFC 3704) mais elles sont peu déployées en pratique. Le projet SAVI ("*Source Address Validation Improvement*") vise à propose des mécanismes pour rendre plus difficile l'utilisation d'adresses IP usurpées. Ce document est son cadre général, exposant les principes.

Les attaques possibles sont documentées dans le RFC 6959, qui explique la portée du projet SAVI. Les deux RFC cités plus haut, collectivement connus sous le nom de « BCP 38 <http://www.bortzmeyer.org/bcp38.html> » (RFC 2827 et RFC 3704), assurent, lorsqu'ils sont déployés, une validation de la source avec pour granularité celle d'un **préfixe** IP. Ainsi, un FAI dont les adresses IP sont en 2001:db8:1::/32 peut empêcher un de ses clients de sortir avec l'adresse 2001:db8:9fe:43::1 (qui n'est pas dans le même préfixe) mais BCP 38 ne traite pas le cas où le client 2001:db8:1:2::42 veut usurper 2001:db8:1:2:73:66:e5: (même préfixe). Il existe des mécanismes privés pour traiter ce cas (comme le "*Source Guard*" de Cisco) mais pas encore de norme. C'est le but de SAVI.

Son principe (section 2) est que tout est fait dans le réseau, pas dans les machines (puisque celles-ci peuvent être sous le contrôle d'un méchant). Il y a trois étapes dans une validation SAVI :

— Déterminer les adresses IP légitimes pour une machine,

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

— Attacher ces adresses IP à une propriété au niveau 2, propriété qui doit être difficile à usurper. Cela peut être par exemple le port physique du commutateur.
— Tester que les paquets ayant cette adresse source obéissent bien à cette propriété.

C'est vague ? Parce que ce n'est qu'un modèle. D'autres RFC, par exemple le RFC 6620, spécifieront rigoureusement cet attachement entre une adresse IP et une propriété de la couche 2. Le RFC 6620 prévoit que le commutateur note les adresses IP source utilisées et refuse ensuite les paquets ayant cette adresse source (le principe est donc « premier arrivé, premier servi ») sauf si un test montre que l'adresse n'est plus joignable sur l'ancien port.

L'entité qui accomplit les trois étapes ci-dessus est appelée « instance SAVI ». Dans l'exemple donné, c'est le commutateur mais cela peut aussi être un routeur ou un autre équipement. C'est typiquement le commutateur qui est le mieux placé pour vérifier les adresses locales (le routeur a du mal à empêcher une machine d'usurper l'adresse d'une autre machine du même lien). Le principe de base est que SAVI est d'autant mieux mis en œuvre qu'on est proche de la source des paquets. Si on s'éloigne :

— Il est plus difficile de déterminer les adresses légitimes,
— On n'a plus de propriétés de niveau 2 à attacher à une adresse,
— On protège moins puisque la machine menteuse pourra toujours parler aux machines proches.

Toutefois, SAVI prévoit le cas où on ne peut pas utiliser la solution idéale (par exemple parce que le commutateur où sont connectées les machines est pré-SAVI et ne gère pas ce RFC), et où on se contente d'une solution imparfaite. Notez qu'un certain nombre de commutateurs ont déjà des fonctions analogues à SAVI, mais de manière non-standard.

La section 3 couvre ces options de déploiement. Toute solution SAVI concrète va dépendre du mécanisme d'allocation d'adresses (le RFC 7513 couvre le cas de DHCP et le RFC 6620 celui des adresses auto-attribuées, par exemple via le RFC 4862) et des caractéristiques de la couche 2. Pour le mécanisme d'allocation d'adresse, il faut noter que plusieurs mécanismes peuvent coexister sur un même lien (section 6).

Pour l'attachement d'une adresse IP à une propriété de couche 2, on a le choix :

— Adresse MAC (déconseillé par le RFC car trop facile à usurper),
— Port physique du commutateur (attention, il peut y avoir plusieurs machines derrière un port),
— Association de sécurité WPA entre une machine et sa base, pour un lien WiFi,
— Identifiant d'une session PPP,
— Identifiant du tunnel, si la machine est connectée via GRE, MPLS, etc.

Chacun de ces cas va nécessiter une incarnation concrète des principes de ce RFC 7039.

Comme souvent en sécurité, le déploiement de la sécurisation va créer de nouveaux problèmes et de nouveaux motifs de panne. La section 5 en expose certains. Par exemple, un commutateur qui mémorise une association adresse¡-¿port et qui redémarre perd ces associations et va alors se mettre à refuser tous les paquets, avant de réapprendre les associations. Ou bien une machine change brusquement de port et, pendant un moment, ne peut plus communiquer. SAVI doit donc prévoir des mécanismes de rattrapage, par exemple, lorsque beaucoup de paquets sont refusés, tester si l'adresse IP est unique sur le lien et, si oui, en déduire que c'était bien la machine légitime qui émettait. (À noter que ces mécanismes sont mis en défaut si la machine légitime était éteinte à ce moment.)

Comme noté par la section 7, une machine SAVI a aussi intéret à connaître le préfixe IP légitime du lien, pour faire un test supplémentaire de validité. Elle peut le faire par configuration explicite, en écoutant les annonces RA ("*Router Advertisment*") du routeur IPv6, en écoutant les messages DHCP de délégation de préfixe, ...(RFC 7513)

N'espérez pas de miracle de SAVI. La section 10, qui résume l'analyse de sécurité, note bien que SAVI rend l'usurpation plus difficile mais ne « prouve » pas l'adresse IP source, au sens où une signature cryptographique prouve l'authenticité d'un document, par exemple. Si on veut faire mieux, il

faut passer à des protocoles avec authentification cryptographique de la source (comme HIP <http://www.bortzmeyer.org/hip-resume.html>).

Notez que SAVI a une longue histoire à l'IETF, chaude et contestée. Le projet se nommait auparavant SAVA ("*Source Address Validation Architecture*", cf. RFC 5210) et avait des objectifs bien plus ambitieux, au point de faire peur à beaucoup, d'autant plus que les propositions venaient de Chine. L'ancien SAVA prévoyait un cadre englobant tout l'Internet, avec intégration de « BCP 38 <http://www.bortzmeyer.org/bcp38.html> » (RFC 2827 et RFC 3704) et communication entre opérateurs pour garantir la validation de bout en bout. À la réunion IETF de Prague en 2008, SAVA s'était fait chaudement allumer. Personne n'avait osé le dire tout haut pendant la réunion mais la salle bruissait de « on ne va pas changer l'architecture de l'Internet pour faire plaisir aux communistes ». Le seul orateur à mentionner ce problème l'avait fait diplomatiquement en disant que SAVA risquait d'amener dans Internet des préoccupations qui sont traditionnellement celles des telcos (comme la facturation à l'usage). SAVI est donc désormais la version "*light*", plus focalisée du point de vue technique, et avec acceptation du fait que tout le monde n'a pas envie d'être fliqué (SAVI soulève quand même plein de problèmes pour la vie privée, qui ne sont pas traités dans ce RFC).