RFC 6506 : Supporting Authentication Trailer for OSPFv3

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 14 février 2012

Date de publication du RFC : Février 2012

https://www.bortzmeyer.org/6506.html

La version 2 du protocole de routage OSPF avait un mécanisme d'authentification (annexe D du RFC 2328 [1]). Lors de la conception de la version 3 (qui permettait notamment d'ajouter IPv6), ce mécanisme avait été abandonné, l'idée étant que l'IETF avait déjà un mécanisme d'authentification plus général, IPsec, et qu'il « suffisait » de l'utiliser. Selon cette analyse, il n'y avait plus besoin de doter chaque protocole de son propre mécanisme d'authentification. C'était très bien sur le papier. Mais, en pratique, le déploiement d'IPsec est très limité, à la fois en raison de sa complexité et du caractère imparfait de ses implémentations. Résultat, les utilisateurs d'OPSFv3 n'ont, la plupart du temps, pas déployé de mécanisme de sécurité du tout. En voulant faire trop propre, on a donc **diminué** la sécurité du routage. Ce RFC (depuis remplacé par le RFC 7166) corrige le tir en dotant enfin OSPFv3 d'un mécanisme d'authentification léger et réaliste.

OSPFv3 est normalisé dans le RFC 5340, dont le titre (« OSPF pour IPv6 ») est trompeur car, depuis le RFC 5838, OSPFv3 peut gérer plusieurs familles d'adresses et peut donc, en théorie, remplacer complètement OSPFv2. En pratique, toutefois, ce n'est pas encore le cas, notamment pour le problème de sécurité qui fait l'objet de ce RFC : contrairement aux autres protocoles de routage internes, OSPFv3 ne disposait d'aucun mécanisme d'authentification. N'importe quel méchant sur le réseau local pouvait se proclamer routeur et envoyer de fausses informations de routage. L'argument répété était « pas besoin de mécanisme spécifique à OSPFv3, utilisez les mécanismes IPsec, comme expliqué dans le RFC 4552 ». Mais on constate que cette possibilité a été très peu utilisée. Le RFC se contente de noter que c'est parce que IPsec est mal adapté à certains environnements comme les MANET mais il ne parle pas des autres environnements, où IPsec est simplement rejeté en raison de la difficulté à trouver une implémentation qui marche, et qu'un administrateur système normal arrive à configurer.

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc2328.txt

IPsec a également des faiblesses plus fondamentales pour des protocoles de routage comme OSPF. Ainsi, les protocoles d'échange de clés comme IKE ne sont pas utilisables tant que le routage ne fonctionne pas. Pour résoudre le problème d'œuf et de poule, et parce que les communications OSPF sont de type un-vers-plusieurs (et pas un-vers-un comme le suppose IKE), le RFC 4552 prône des clés gérées manuellement, ce qui n'est pas toujours pratique.

Enfin, l'absence de protection contre le rejeu affaiblit la sécurité d'IPsec dans ce contexte, comme le note le RFC 6039.

La solution proposée figure en section 2. L'idée est d'ajouter à la fin du packet OSPF un champ qui contienne un condensat cryptographique du paquet et d'une clé secrète, comme pour OSPFv2 (RFC 5709) (D'autres types d'authentification pourront être utilisés dans le futur, un registre IANA des types <https://www.iana.org/assignments/ospfv3-authentication-trailer-options/ospfv3-authent xml> a été créé.) Les options binaires du paquet, au début de celui-ci (RFC 5340, section A.2), ont un nouveau bit, en position 13, AT (pour "*Authentication Trailer*", désormais dans le registre IANA <https://www.iana.org/assignments/ospfv3-parameters/ospfv3-parameters.xml#ospfv3-parameters-1>) qui indique la présence ou l'absence du champ final d'authentification (tous les paquets n'ont pas ce champ Options, donc le routeur devra se souvenir des valeurs de ce champ pour chaque voisin).

Pour chaque couple de routeurs ainsi protégés, il y aura un certain nombre de paramètres, qui forment ce qu'on nomme un accord de sécurité ("*security association*", section 3) :

— Un identifiant sur 16 bits, manuellement défini, le "*Security Association ID*". L'émetteur le choisit et le récepteur le lit dans le paquet. Cette indirection va permettre de modifier des paramètres comme les clés cryptographiques (ou même l'algorithme cryptographique), tout en continuant le routage.
— L'algorithme utilisé, par exemple HMAC-SHA1 ou HMAC-SHA512,
— La clé,
— Des paramètres temporels indiquant, par exemple, à partir de quand la clé sera valide.

Une fois qu'on a toutes ces informations, qu'est-ce qu'on met dans le paquet OSPF envoyé sur le câble ? La section 4 décrit le mécanisme. Le champ final d'authentification ("*Authentication Trailer*") est composé notamment de l'identifiant d'un accord de sécurité (SA ID, décrit au paragraphe précédent, et qui permet au récepteur de trouver dans sa mémoire les paramètres cryptographiques liés à une conversation particulière), d'un numéro de séquence (qui sert de protection contre le rejeu ; il est augmenté à chaque paquet émis ; il comprend 64 bits, après une très longue discussion dans le groupe de travail, certains auraient préféré 32 bits) et du condensat cryptographique du paquet concaténé avec la clé (la section 4.5 décrit l'algorithme en détail et notamment quels champs du paquet sont inclus dans les données condensées).

Le routeur qui reçoit un paquet utilisant l'authentification (il le sait grâce au bit AT qui était notamment présent dans les paquets OSPF Hello) va accéder au champ d'authentification (le champ Longueur du paquet OSPF lui permet de savoir où commence le champ d'authentification, éventuellement en tenant compte du bloc "*Link-Local Signaling*" du RFC 5613, un routeur doit donc gérer au moins en partie ce dernier RFC s'il veut authentifier). Le récepteur refait alors le calcul cryptographique et vérifie si le champ final d'authentification est correct. Le calcul est très proche de celui du RFC 5709 à part l'inclusion de l'adresse IPv6 source.

Supposons que nous soyons administrateur réseaux et que nos routeurs gèrent tous ce nouveau RFC. Comment déployer l'authentification sans tout casser ? La section 5 recommande de migrer tous les routeurs connectés au même lien simultanément. Autrement, les routeurs qui n'utilisent pas l'authentification ne pourront pas former d'adjacences OSPF avec ceux qui l'utilisent. Le RFC prévoit un mode de transition, où le routeur envoie le champ final d'authentification mais ne le vérifie pas en entrée mais l'implémentation de ce mode n'est pas obligatoire.

La section 6 contient l'analyse de sécurité de cette nouvelle extension d'OSPF. Elle rappelle qu'elle ne fournit **pas** de confidentialité (les informations de routage seront donc accessibles à tout espion). Son seul but est de permettre l'authentification des routeurs, résolvant les problèmes notés par le RFC 6039. À noter que cette extension ne permet pas d'authentifier **un** routeur particulier mais simplement de s'assurer que l'émetteur est autorisé à participer au routage sur ce lien (tous les routeurs ont la même clé). La clé, rappelle cette section 6, devrait être choisie aléatoirement, pour ne pas être trop facile à deviner (cf. RFC 4552).

À ma connaissance, il n'existe pas encore d'implémentation de cette option dans le logiciel d'un routeur.