RFC 6863 : Analysis of OSPF Security According to KARP Design Guide

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 2 mars 2013

Date de publication du RFC : Mars 2013

https://www.bortzmeyer.org/6863.html

Le projet **KARP** ("*Keying and Authentication for Routing Protocols*") vise à améliorer la sécurité des communications entre routeurs. La toute première étape est d'analyser l'état actuel de cette sécurité et ce RFC le fait pour le cas du protocole OSPF.

Il suit pour cela les principes posés dans le RFC 6518 [1] dans sa section 4.2, « "*Work Items per Routing Protocol*" ». Le RFC 6039 avait déjà fait une telle analyse sous l'angle de la cryptographie. Des "*Internet-Drafts*" comme `draft-ietf-rpsec-ospf-vuln` ont été écrits sur des aspects plus généraux de la sécurité d'OSPF. Et des travaux ont déjà bien avancés pour améliorer cette sécurité (comme l'ajout de l'authentification à OSPF v3 dans le RFC 6506). Ce nouveau RFC 6863 couvre le reste.

D'abord, la gestion des clés. Celle-ci est manuelle, dans OSPF. C'est à l'administrateur réseaux de choisir les clés, de configurer les routeurs, de changer les clés en allant modifier chaque routeur, etc. Pour un protocole à gestion manuelle, OSPF est plutôt bon : l'intégrité des communications est protégée, le changement d'algorithme cryptographique est possible (ce que l'on nomme l'agilité cryptographique), la sécurité n'empêche pas de prioritiser certains paquets (comme les `HELLO`), etc.

Mais, par rapport aux exigences du RFC 6862, il reste quelque manques, et ce RFC a pour but de les lister. Par exemple :

— OSPF utilise directement les PSK (voir le RFC 6862 pour le vocabulaire), les clés fournies. Il ne fait pas de dérivation, ce qui permet certaines attaques.

1. Pour voir le RFC de numéro NNN, `https://www.ietf.org/rfc/rfcNNN.txt`, par exemple `https://www.ietf.org/rfc/rfc6518.txt`

— Les protections contre les attaques par rejeu sont inexistantes en OSPF v3 et insuffisantes en v2. Notez qu'il existe des attaques à l'intérieur d'une session OSPF établie (le RFC dit "*intra-connection*") et d'autres en dehors d'une session (attaques "*inter-connections*").
— OSPF v3 n'avait pas d'autre sécurité qu'IPsec. Mais IPsec interfère sérieusement avec la priorisation des paquets. On souhaite typiquement que les paquets `HELLO`, indispensables au maintien de la session, aient la priorité. Mais s'ils sont chiffrés avec IPsec, ce n'est plus possible, tous les paquets doivent être traités par IPsec, avant qu'on puisse les identifier et donc les prioritiser.
— L'identification du voisin ne se fait dans certains cas qu'avec l'adresse IP, ce qui n'est pas suffisant pour la sécurité.

Si vous voulez un résumé de la sécurité dans OSPF, la section 2 du RFC est faite pour vous, elle détaille l'état actuel, et les faiblesses. Rappelez-vous qu'il existe deux versions d'OSPF en service, OSPF v2 (RFC 2328), probablement le plus fréquent dans la nature, et OSPF v3 (RFC 5340 et RFC 5838) qui n'a pas été un grand succès.

D'abord, OSPF v2. L'annexe D du RFC 2328 décrit son mécanisme de protection cryptographique. En gros, on prend la plupart des champs de l'en-tête du paquet (mais pas l'adresse IP), plus un secret, on les condense et on ajoute le MAC au paquet. À l'époque, la fonction de condensation était forcément du MD5. Le RFC 5709 a permis des algorithmes modernes comme la famille SHA-2. Notez que la cryptographie n'est pas sans défauts (section 7) : comme elle impose des calculs importants à des engins qui n'ont pas forcément de gros processeurs, elle fournit une voie d'attaque par déni de service. Des protections supplémentaires comme celle du RFC 5082, permettant d'empêcher un attaquant extérieur d'injecter des paquets, sont à considérer.

OSPF v2 a une protection limitée contre le rejeu. Les paquets comportent un numéro de séquence qui est croissant. Il n'est donc pas possible de rejouer un vieux paquet, son numéro de séquence trop bas le trahirait. Mais il y a quelques limites : la norme impose que le numéro ne décroisse jamais, mais n'oblige pas à l'incrémenter à **chaque** paquet. Et elle ne précise rien sur le numéro initial (au démarrage du routeur) donc certains risquent de choisir un numéro initial identique à chaque démarrage (par exemple, avoir un numéro de séquence qui soit purement et simplement le nombre de secondes écoulées depuis le démarrage du routeur est tout à fait compatible avec la norme, mais très peu sûr). Autre piège, l'adresse IP n'est pas incluse dans la somme de contrôle, donc un attaquant peut copier un paquet envoyé par un pair, changer l'adresse IP et se faire ainsi passer pour un autre pair.

Par contre, OSPF v2 est tout à fait satisfaisant pour ce qui concerne le remplacement des clés. Les clés ont un identificateur, et des durées de vie explicitement indiquées (annexe D.3 du RFC 2328, qui permet d'accepter une nouvelle clé avant de l'utiliser soi-même), ce qui permet de faire des remplacements propres des clés.

Et OSPF v3 ? Malgré son numéro de version supérieur, il était plutôt moins bien placé, question sécurité. L'idée avait été de ne plus mettre de fonctions de sécurité dans OSPF, mais de compter sur IPsec pour tout (RFC 4552). IPsec fournissait tous les services demandés (et même d'autres comme la confidentialité), avec les caractéristiques souhaitées (comme l'agilité cryptographique). Mais IPsec ayant été très peu déployé, les sessions OSPF v3 se retrouvaient en pratique toutes nues. (Il y avait aussi des problèmes moins graves comme le fait que le chiffrement IPsec empêchait de prioritiser certaines paquets OSPF, puisqu'il fallait tout déchiffrer dans l'ordre d'arrivée avant de savoir lesquels étaient prioritaires. Même sans chiffrement, les techniques d'encapsulation d'IPsec rendaient l'analyse des paquets entrants difficile.)

La section 3 revient plus en détail sur les problèmes de rejeu. Aucune des deux versions d'OSPF n'est parfaite sur ce plan mais OSPF v3 est nettement plus vulnérable.

Après cet examen de l'existant, la section 4 résume ce qui manque à OSPF :

— Meilleure protection contre le rejeu,
— Inclure l'en-tête IP, notamment l'adresse source, dans la partie protégée du paquet,
— Fournir une solution d'authentification à OSPF v3, ne nécessitant pas IPsec (cela a été fait dans le RFC 6506).

La section 5 pose ensuite les étapes du travail :

— Spécifier un mécanisme où le numéro de séquence est séparé en deux parties, une stockant un nombre qui s'accroit à chaque redémarrage du routeur (et doit donc être stocké sur un support stable, ce qui n'est pas évident pour tous les routeurs) et une strictement croissante depuis le démarrage. Cela garantira que le numéro de séquence ne décroit jamais, même en cas de redémarrage.
— Décrire un mécanisme de dérivation de clés, de manière à éviter qu'une clé utilisée pour OSPF et un autre protocole ne fasse tomber les deux protocoles, en cas de compromission.
— Et divers autres mécanismes à normaliser (ce travail est déjà bien avancé, dans l'"*Internet-Draft*" `ietf-ospf-security-extension-manual-keying`).