RFC 6094 : Summary of Cryptographic Authentication Algorithm Implementation Requirements for Routing Protocols

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 3 février 2011

Date de publication du RFC : Février 2011

https://www.bortzmeyer.org/6094.html

Plusieurs protocoles de routage utilisent de la cryptographie pour l'authentification. C'est le cas par exemple d'OSPFv2 (RFC 2328 [1]), IS-IS (RFC 1195) et RIP (RFC 2453). Limitée au début à MD5, la liste des algorithmes utilisées croît petit à petit mais dans le désordre. L'idée de ce RFC est de spécifier le minimum d'algorithmes qu'un routeur sérieux doit gérer, de manière à garantir l'interopérabilité. Il faut être sûr que tous les routeurs aient au moins un algorithme en commun.

La section 1 détaille le problème. Lorsque qu'un protocole de routage (prenons comme exemple OSPFv2, RFC 2328, annexe D) permet d'authentifier ses pairs, il peut le faire par un mot de passe passé en clair, ou bien par un condensat cryptographique du mot de passe et d'autres informations. (D'autres protocoles sous-traitent l'authentification à une couche inférieure, comme OSPFv3 - RFC 5340 - qui la délègue à IPsec mais ils sont hors-sujet pour ce RFC. Depuis le RFC 6506, OSPFv3 a de toute façon une authentification à lui.) Le mot de passe en clair offre peu de sécurité puisque n'importe quel "*sniffer*" peut le capter. Ce mot de passe n'est vraiment efficace que contre les accidents, pas contre les attaques délibérées. La protection par condensat cryptographique n'a pas cet inconvénient. Elle fonctionne en résumant un message composé d'un secret partagé (le mot de passe) et d'autres informations connues des routeurs. Ainsi, le mot de passe ne circule jamais en clair.

Traditionnellement, la fonction de hachage utilisée était MD5 (RFC 1321) mais des attaques cryptographiques réussies contre MD5 mènent à son abandon progressif. L'avantage de MD5 était que tout le monde le connaissait et l'utilisait, alors que la migration vers de nouveaux algorithmes fait courir un risque de babelisation. Il faut noter que les attaques connues contre MD5 (RFC 4270) ne s'appliquent

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

pas forcément à l'utilisation qu'en font les protocoles de routage et que la vulnérabilité de MD5 est donc encore dans le futur. Néanmoins, il est plus prudent de prévoir son remplacement dès aujourd'hui. Les remplaçants envisagés sont en général de la famille SHA. Ceux-ci seront sans doute à leur tour remplacés dans le futur, la cryptanalyse ne cessant jamais de progresser. L'ancienne normalisation, qui indiquait « en dur » la fonction de hachage dans la spécification du protocole de routage, n'est donc plus adaptée. Les sections suivantes du RFC détaillent la situation pour les principaux protocoles de routage cherchant, pour chacun d'eux, comment éliminer MD5 tout en ayant un algorithme commun.

Commençons par la section 2, consacrée à IS-IS. Si la norme ISO originelle ne permettait que le mot de passe en clair, le RFC 5304 a ajouté la possibilité de cryptographie, d'abord avec MD5 puis, dans le RFC 5310, d'autres algorithmes comme la famille SHA. L'avantage de l'authentification par mot de pass en clair est que, normalisée dès le début, elle fonctionne avec toutes les mises en œuvre de IS-IS. Sa sécurité est très mauvaise (il est trivial d'écouter le réseau pour découvrir le mot de passe). Il est donc recommandé d'utiliser les solutions cryptographiques, mais cela implique des algorithmes communs. Si un routeur ne connait que SHA-256 et l'autre que SHA-1, ils ne pourront pas s'authentifier mutuellement. Or, même si les deux routeurs mettent en œuvre le RFC 5310, cette situation est possible.

Notre RFC ne fait pas de choix mais demande que les futurs RFC sur IS-IS choisissent au moins un algorithme obligatoire, qui sera donc connu de tous les routeurs, et qui ne soit pas MD5.

L'autre grand protocole de routage interne, OSPF, fait l'objet de la section 3. Si OSPFv3 reposait entièrement sur IPsec et n'avait pas de mécanisme d'authentification propre (cela a changé avec le RFC 6506), OSPFv2 (de très loin le plus utilisé) a son mécanisme à lui. Ce dernier, dans la norme originale (RFC 2328), permettait le mot de passe en clair ou bien de la cryptographie avec MD5. Le RFC 5709 ajoutait la possibilité d'utiliser la famille SHA. Mais les seuls mécanismes d'authentification obligatoires sont ceux de l'ancien RFC (y compris le plus simple, « pas d'authentification »). Comme avec IS-IS, il est donc nécessaire qu'une nouvelle norme dise clairement quel est l'algorithme standard et sûr que doivent mettre en œuvre tous les logiciels OSPF.

Quant à OSPFv3 (section 4), du fait qu'il utilise IPsec, ses algorithmes communs sont ceux d'IPsec, ESP (RFC 4522) qui lui même utilise SHA-1 (RFC 2404). Ce dernier sera sans doute remplacé bientôt par AES (qui avait été introduit dans le RFC 3566).

Et le bon vieux RIP, dans sa version RIPv2 (section 5) ? Sa norme actuelle est le RFC 2453, qui ne prévoyait comme authentification que le mot de passe en clair. Le RFC 2082 ajoutait MD5 que le RFC 4822 a remplacé par SHA. Toutefois, comme les deux autres protocoles cités, RIP n'a pas d'algorithme unique garanti et une nouvelle norme est donc nécessaire, pour éviter que les routeurs ne se rabattent sur MD5 (ou, pire, sur le mot de passe en clair) pour pouvoir interopérer.

La version RIPng, elle (section 6), comme OSPFv3, se repose entièrement sur IPsec et donc sur les mêmes algorithmes.

La section 7 résume et rappelle les problèmes de sécurité abordés. D'abord, tous les mécanismes étudiés ici ne fournissent que l'authentification. Si on désire en plus de la confidentialité, il faut chercher ailleurs (par exemple IPsec avec ESP). D'autre part, les experts en cryptographie conseillent généralement de changer les clés régulièrement, diverses attaques cryptanalytiques prenant du temps. Il ne faut donc pas en donner à l'ennemi. Or, aucun de ces protocoles de routage ne fournit de mécanisme pour un remplacement coordonné des clés, il faut tout gérer à la main.