

RFC 2385 : Protection of BGP Sessions via the TCP MD5 Signature Option

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 6 Janvier 2009

Date de publication du RFC : Août 1998

<http://www.bortzmeyer.org/2385.html>

Le protocole TCP est vulnérable à plusieurs attaques fondées sur l'envoi de paquets prétendant venir d'un correspondant légitime, alors qu'ils sont injectés dans le réseau par le méchant. La communauté des opérateurs Internet est depuis longtemps particulièrement soucieuse de ces risques pour les sessions BGP entre ses membres et a donc développé ce bricolage qui consiste à insérer une option TCP validant très partiellement les paquets. (Bien que cette vulnérabilité de TCP soit très générale, cette solution n'a été utilisée que pour BGP. Le résultat est un très court RFC, traitant - assez mal - un problème très particulier.)

Une attaque typique contre BGP est une DoS où le méchant envoie un paquet TCP RST ("*ReSeT*", sections 3.1 et 3.4 du RFC 793¹) qui va couper brutalement la session. Les techniques récentes comme TLS ne protègent pas contre ce genre d'attaques car elle opèrent juste en dessous de la couche application, et ne peuvent pas authentifier les paquets TCP (section 1). Même chose si on avait une solution purement BGP.

La solution de ce RFC est donc (section 2) d'insérer dans chaque **segment** TCP un résumé cryptographique MD5 portant sur une partie des en-têtes IP et TCP, les données, **et** un secret partagé entre les deux routeurs. L'attaquant ne connaissant pas ce mot de passe, il ne peut pas fabriquer de faux paquets.

À noter que, bien qu'enregistrée dans le registre IANA des options <<http://www.iana.org/assignments/tcp-parameters/tcp-parameters.xml>>, ce n'est pas une « vraie » option TCP :

1. Pour voir le RFC de numéro NNN, <http://www.ietf.org/rfc/rfcNNN.txt>, par exemple <http://www.ietf.org/rfc/rfc793.txt>

les options TCP (section 3.1 du RFC 793) ne sont pas, comme leur nom l'indique, obligatoires. Chacun des deux pairs peut les refuser. Ici, pour éviter toute attaque par repli, la signature TCP MD5 est à prendre ou à laisser.

Passons aux bits sur le câble, avec la section 3 qui décrit le format dans le paquet. Puis aux considérations pratiques avec la section 4 qui détaille les problèmes qui peuvent se produire avec les signatures MD5, comme les soucis qui peuvent provenir car des paquets TCP légitimes peuvent être refusés (section 4.1 mais qui ne mentionne pas le fait que des paquets ICMP, non validés par la signature MD5, peuvent par contre être acceptés alors qu'ils sont faux), le coût en performance à cause des opérations cryptographiques (section 4.2 mais il faut relativiser : lorsque le RFC a été écrit, l'exemple de processeur de routeur était le MIPS R4600, à 100 Mhz) ou l'augmentation de la taille des paquets (section 4.3).

Plus sérieux est le problème de la vulnérabilité de MD5. Elle était déjà bien connue à l'époque (section 4.4) et ça ne s'est évidemment pas arrangé. (En décembre 2008, une attaque réussie contre MD5 <<http://www.freedom-to-tinker.com/blog/felten/researchers-show-how-forge-site-certificates>> a permis de générer de faux certificats X.509). À noter que le RFC ne prévoit pas de moyen d'indiquer un autre algorithme cryptographique que MD5, pour les raisons expliquées dans cette section 4.4. De l'avis de certains <<http://mailman.nanog.org/pipermail/nanog/2009-January/006408.html>>, dans le cas de BGP, MD5 reste encore relativement raisonnable. Néanmoins, cela ne pouvait pas durer éternellement et c'est l'une des motivations qui ont finalement mené au remplacement de ce protocole (cf. RFC 5926).

Presque tous les routeurs dédiés savent utiliser cette option MD5 TCP. Ainsi, sur IOS, c'est le mot-clé "password" :

```
router bgp 64542
  neighbor 192.0.2.108 password g2K1R43Ag
```

La situation est plus délicate sur les routeurs non-dédiés, par exemple fondés sur Unix. Linux ou FreeBSD n'ont pas eu pendant longtemps le support du RFC 2385 en série (il existait des "patches" comme <<http://hasso.linux.ee/doku.php/english:network:rfc2385>>), en partie pour une question de principe <<http://lkml.indiana.edu/hypertext/FAQs/FAQkernel/0203.1/1133.html>> (cette option viole le modèle en couches avec ses aller-retours entre l'application et TCP). (Pour Quagga, voir certains liens en <<http://wiki.quagga.net/index.php/Main/AddRes>>.) Aujourd'hui, le noyau Linux (par exemple en version 2.6.26) a cette fonction (au moment de la compilation, activer "TCP : MD5 Signature Option support (RFC2385) (EXPERIMENTAL)", ce qui est le cas sur Debian par défaut).

En pratique, l'exigence de sessions « TCP MD5 » a souvent servi à éliminer ceux qui utilisent Quagga sur Unix et n'avaient pas de moyen facile de configurer leurs routeurs selon cette option.

Une autre objection fréquente faite à ce RFC 2385 est qu'il aurait mieux valu utiliser IPsec, qui a l'avantage de couvrir les autres protocoles (comme ICMP) et d'être plus générique. Mais IPsec, notamment en raison de sa complexité, a connu peu de déploiements.

Le groupe de travail tcpm <<http://tools.ietf.org/wg/tcpm>> de l'IETF a donc finalement développé un meilleur protocole, "TCP Authentication Option (TCP-AO)", normalisé dans le RFC 5925.

Un bon exposé technique en français sur ce RFC est dans l'article « Les signatures MD5 des segments TCP <<http://www.hsc.fr/ressources/breves/tcp-md5.html.fr>> ».