RFC 6952 : Analysis of BGP, LDP, PCEP and MSDP Issues According to KARP Design Guide

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 25 mai 2013

Date de publication du RFC : Mai 2013

https://www.bortzmeyer.org/6952.html

Dans le cadre du travail du groupe KARP <http://tools.ietf.org/wg/karp> de l'IETF, consacré à la sécurisation des protocoles de routage de l'Internet, ce RFC est consacré à l'analyse de la sécurité des protocoles de routage utilisant TCP, notamment BGP.

Deux petits rappels : KARP travaille sur les protocoles eux-mêmes, ni sur le contenu des informations transmises (c'est le rôle de SIDR <http://tools.ietf.org/wg/sidr>, qui a produit le système RPKI+ROA <https://www.bortzmeyer.org/securite-routage-bgp-rpki-roa.html>), ni sur les pratiques quotidiennes d'administration des routeurs. Son rôle est d'améliorer la sécurité des protocoles, et pour cela il commence par des analyses de la sécurité des protocoles existants, suivant une méthode décrite dans le RFC 6518 [1]. Il y avait déjà eu une analyse d'OSPF (RFC 6863) et ce nouveau RFC s'attaque à des protocoles très différents mais qui ont en commun d'utiliser TCP comme transport : BGP (RFC 4271) et LDP (RFC 5036), ainsi que les moins connus PCEP ("*Path Computation Element Communication Protocol*", RFC 5440) et MSDP (RFC 3618). Ils appartiennent tous à la catégorie un-vers-un du RFC 6518 (les messages d'un routeur sont transmis à un seul autre routeur).

Donc, aujourd'hui, quels sont les risques de sécurité pour ces protocoles et les défenses existantes ? D'abord, ceux et celles spécifiques à la couche transport. Il y a les attaques par déni de service et les attaques où l'ennemi va tenter d'établir une session avec sa victime, sans en avoir normalement le droit. Parmi les contre-mesures (RFC 4732 pour un point de vue plus général), il y a des ACL par adresse IP (tous ces protocoles utilisant TCP, il n'y a normalement pas de possibilité pour un attaquant en dehors du chemin d'usurper une adresse IP, si tout le monde suit bien le RFC 4953 et le RFC 5961) et le fait d'écouter les connexions entrantes uniquement sur les interfaces où on s'attend à avoir des pairs. Pour

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

éviter les attaques de méchants lointains, il y a la technique GTSM du RFC 5082, qui consiste à n'accepter des paquets que s'ils ont un TTL maximal (ou proche du maximum).

Cela ne suffit pas contre des assaillants situés sur le chemin (par exemple parce qu'ils sont sur le réseau local). Ceux-ci peuvent établir une connexion avec une fausse adresse IP, ou bien simplement envoyer des "*resets*" TCP pour couper les sessions existantes (notez que TLS ou SSH ne protégeraient **pas** contre ce dernier risque car ils fonctionnent au-dessus de TCP). Pour assurer l'authentification et l'intégrité de la connexion TCP, on a l'« authentification MD5 » du RFC 2385, normalement remplacée par l'AO du RFC 5925. AO est très supérieur, fournissant notamment l'agilité cryptographique (la possibilité de changer d'algorithme si la cryptanalyse en a trop affaibli un, ce qui est le cas de MD5). Mais AO est loin d'avoir remplacé MD5.

Et puis il y a les problèmes qui ne dépendent pas du transport utilisé, comme l'absence d'un protocole de gestion des clés (KMP pour "*Key Management Protocol*"). Actuellement, la gestion des clés dans tous ces protocoles est purement manuelle et, résultat, les clés cryptographiques des routeurs ne sont quasiment jamais changées, même lorsqu'un administrateur quitte la société.

Maintenant, place à chaque protocole individuellement. Le RFC fait une présentation de chaque protocole (section 2), puis de l'état de sécurité idéal qu'on souhaite atteindre (section 3), puis de la différence entre l'état actuel et cet idéal (section 4). Enfin, la section 5 étudie les questions de transition vers une meilleure solution de sécurité (tous ces protocoles étant pair-à-pair, il faut que les deux pairs soient d'accord pour la nouvelle technique de sécurité). Ici, je procède différemment en traitant tous les aspects de chaque protocole successivement (enfin, pas chacun, je ne couvre que BGP et LDP, ne connaissant pas vraiment PCEP et MSDP). Donc, honneur à BGP pour commencer, puisque c'est sans doute le protocole de routage le plus important pour l'Internet (section 2.3). Comme il ne fonctionne que sur TCP, sa sécurité est en bonne partie celle de ce protocole de transport. Autrement, il devra attendre le déploiement d'AO, puis d'un KMP pour que sa sécurité s'améliore.

LDP, lui, est utilisé par MPLS et le RFC général de sécurité sur MPLS, le RFC 5920 est donc une utile lecture, ainsi que la section 5 du RFC 5036. LDP (sections 2.4, 3.1 et 4.1 de notre RFC) peut, lui, fonctionner sur TCP ou sur UDP. Ce dernier sert notamment aux messages `Hello` d'établissement d'une session. Cet établissement n'est donc pas protégé par les mesures de sécurité de TCP. En fait, il n'existe même quasiment aucune protection pour ces messages. Et pour TCP ? LDP peut utiliser l'authentification MD5 du RFC 2385 mais on a vu que MD5 n'était pas conseillé (RFC 6151 et section 2.9 du RFC 5036) et LDP ne permet pas encore d'utiliser AO (RFC 5925).

L'état de sécurité idéal pour LDP serait clairement un état où les messages `Hello` seraient authentifiés. En attendant, les contre-mesures minimales sont de n'accepter des `Hello` que sur les interfaces réseau qui en ont réellement besoin, et d'utiliser GSTM. Cela ne supprime pas toutes les attaques, mais un travail est déjà en cours pour l'authentification des `Hello` ("*Internet-Draft*" `draft-zheng-mpls-ldp-hello-cr`