RFC 5062 : Security Attacks Found Against the Stream Control Transmission Protocol (SCTP) and Current Countermeasures

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 11 octobre 2007

Date de publication du RFC : Septembre 2007

https://www.bortzmeyer.org/5062.html

Ce RFC documente les problèmes de sécurité connus pour le protocole de transport SCTP. Ces problèmes, présents dans la première version de la norme, le RFC 2960[1], documentés une première fois dans le RFC 4460, sont traités dans la dernière version de la norme, le RFC 4960.

SCTP est très peu utilisé par rapport à son grand concurrent TCP. S'il règle certaines failles de sécurité de celles-ci (par exemple en intégrant un mécanisme d'authentification des adresses IP plus robuste pour l'établissement de la connexion), ses nouvelles possibilités pour le "*multihoming*" ouvrent des nouvelles failles.

Celles-ci, d'abord discutées dans le RFC 4460, sont désormais documentées dans le RFC 4960, qui change légèrement le protocole et donne plusieurs conseils aux implémenteurs. Bien que SCTP ne se place pas réellement dans la catégorie des protocoles à séparation de l'identificateur et du localisateur <https://www.bortzmeyer.org/separation-identificateur-localisateur.html>, ces faiblesses sont quand même proches de celles trouvées dans ces protocoles : l'ajout d'un niveau d'indirection supplémentaire permet de nouvelles usurpations. Avec SCTP, le fond du problème est qu'un attaquant peut dire la vérité sur l'adresse IP principale, celle qui sert à établir la connexion (SCTP dit l'**association**), mais mentir sur les adresses IP supplémentaires.

Par exemple, la première attaque documentée (section 2), le **camping**, consiste pour un attaquant à se connecter à un serveur en annonçant des adresses IP supplémentaires, qui ne sont pas à lui, et, en

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc2960.txt

« campant » ainsi dessus, il peut empêcher leur légitime titulaire d'établir une association avec le même serveur.

La solution proposée par le RFC est de tester ces adresses (ce qui était déjà prévu par le mécanisme de **battement de cœur** dans le RFC 2960 mais sans l'utiliser pour la sécurité). On notera que ce test empêche d'utiliser ces adresses IP supplémentaires si elles ne sont pas joignables immédiatement par la machine associée. C'est conforme au cahier des charges de SCTP, qui vise le "*multihoming*", pas la mobilité (un RFC séparé, le RFC 5061 fournit des pistes pour mieux gérer la mobilité).

Une autre attaque documentée (section 5) est le bombardement, qui permet des DoS. L'attaquant prétend contrôler une adresse IP (en fait, celle de sa victime), établit l'association en indiquant cette adresse IP comme supplémentaire et demande un gros transfert de données, qui frappera sa victime. Si celle-ci n'a **pas** SCTP, elle ne pourra pas signaler l'erreur. Là encore, la solution est de tester toute adresse IP avant de lui envoyer des données.