RFC 8261 : Datagram Transport Layer Security (DTLS) Encapsulation of SCTP Packets

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 16 novembre 2017

Date de publication du RFC : Novembre 2017

https://www.bortzmeyer.org/8261.html

Le protocole de transport SCTP est normalement prévu pour tourner directement sur IP. Pour diverses raisons, il peut être utile de le faire tourner sur un autre protocole de transport comme UDP (ce que fait le RFC 6951 [1]) ou même sur un protocole qui offre des services de sécurité comme DTLS (ce que fait notre nouveau RFC).

SCTP est défini dans le RFC 4960. C'est un concurrent de TCP, offrant un certain nombre de services que TCP ne fait pas. DTLS, normalisé dans le RFC 6347, est un protocole permettant d'utiliser les services de sécurité de TLS au-dessus d'UDP. Il est notamment très utilisé par WebRTC (RFC 8827), lui donnant ainsi une sécurité de bout en bout.

En théorie, SCTP peut fonctionner directement sur IP. Hélas, dans l'Internet actuel, très ossifié, plein d'obstacles s'y opposent. Par exemple, les routeurs NAT tel que la "*box*" de M. Michu à la maison, n'acceptent en général que TCP et UDP. Et bien des pare-feux bloquent stupidement les protocoles que leurs auteurs sont trop ignorants pour connaître. En pratique, donc, SCTP ne passe pas partout. L'encapsuler dans un autre protocole de transport, comme UDP (directement, ou bien via DTLS), est souvent la seule solution pour avoir une connectivité. L'intérêt de DTLS est qu'on a toute la sécurité de TLS, notamment la confidentialité via le chiffrement.

Cette encapsulation est simple (section 3) : on met le paquet SCTP, avec ses en-têtes et sa charge utile, dans les données du paquet DTLS.

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc6951.txt

Il y a toutefois quelques détails à prendre en compte (section 4 de notre RFC). Par exemple, comme toute encapsulation prend quelques octets, la MTU diminue. Il faut donc un système de PMTUD. Comme l'encapsulation rend difficile l'accès à ICMP (voir la section 6) et que les "*middleboxes*" pénibles dont je parlais plus haut bloquent souvent, à tort, ICMP, cette découverte de la MTU du chemin doit pouvoir se faire sans ICMP (la méthode des RFC 4821 et RFC 8899 est recommandée).

Cette histoire de MTU concerne tout protocole encapsulé. Mais il y a aussi d'autres problèmes, ceux liés aux spécificités de SCTP (section 6) :

— Il faut évidemment établir une session DTLS avant de tenter l'association SCTP (≪ association ≫ est en gros l'équivalent de la connexion TCP),
— On peut mettre plusieurs associations SCTP sur la même session DTLS, elles sont alors identifiées par les numéros de port utilisés,
— Comme DTLS ne permet pas de jouer avec les adresses IP (en ajouter, en enlever, etc), on perd certaines des possibilités de SCTP, notamment le "*multi-homing*", pourtant un des gros avantages théoriques de SCTP par rapport à TCP,
— Pour la même raison, SCTP sur DTLS ne doit pas essayer d'indiquer aux couches inférieures des adresses IP à utiliser,
— SCTP sur DTLS ne peut pas compter sur ICMP, qui sera traité plus bas, et doit donc se débrouiller sans lui.

Cette norme est surtout issue des besoins de WebRTC, dont les implémenteurs réclamaient un moyen facile de fournir sécurité et passage à travers le NAT. Elle est mise en œuvre depuis longtemps, dans des clients WebRTC comme Chrome, Firefox ou Opera.