Le spin bit de QUIC

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 28 mai 2021

https://www.bortzmeyer.org/quic-spin-bit.html

Une bonne partie du travail à l'IETF sur le protocole QUIC <https://www.bortzmeyer.org/quic.html> avait tourné autour d'**un seul bit** de l'en-tête QUIC, le "*spin bit*". Pourquoi ?

Ce bit intéressant apparait dans les paquets QUIC à en-tête court (cf. le RFC 9000[1]), et a agité énormément d'électrons lors des discussions à l'IETF. Pour comprendre ces polémiques, il faut voir à quoi sert ce bit. Avec TCP, quelqu'un qui surveillait le réseau pouvait calculer un certain nombre de choses sur la connexion TCP, comme le RTT, par exemple, en observant le délai entre un octet et l'accusé de réception couvrant cet octet. Cela peut être utilisé pour régler le réseau de manière à améliorer les performances (mais ne rêvez pas : contrairement à ce qui a parfois été prétendu, aucun FAI ne va vous informer de la santé de vos connexions individuelles, ni vous aider à les optimiser). Mais c'est également un problème de vie privée (toute information que vous envoyez sur le réseau peut être utilisée à mauvais escient). L'une des idées fortes de QUIC est de réduire la vue présentée au réseau (RFC 8546) et donc de chiffrer au maximum ; avec QUIC, on ne peut plus trouver le RTT en examinant les paquets qui passent. Cela peut être un problème si on souhaite justement informer le réseau et les gens qui le gèrent. Le "*spin bit*" a donc pour but de donner un minimum d'informations explicitement (alors qu'avec TCP, on donne plein d'informations sans s'en rendre compte). Ce "*spin bit*" est public (il n'est pas dans la partie chiffrée du paquet) et est inversé par l'initiateur de la connexion à chaque aller-retour (section 17.4 du RFC). Cela permet donc d'estimer le RTT. Cette utilisation est par exemple mise en œuvre dans le programme spindump <https://github.com/EricssonResearch/spindump>.

Ce "*spin bit*" est optionnel, puisqu'on a vu qu'il pouvait être mal utilisé. Le RFC précise qu'une mise en œuvre de QUIC doit permettre sa désactivation, globalement ou par connexion. Il ajoute que, même si le "*spin bit*" est activé, QUIC doit le débrayer pour au moins une connexion sur seize, choisie au hasard, pour que les gens qui veulent être discrets et donc coupent le "*spin bit*" ne soient pas trop séparables des autres. C'est un principe classique en protection de la vie privée : il ne faut pas se distinguer. Pendant une enquête de police, les gens qui ont éteint leur ordiphone peu avant les faits seront les premiers suspects…

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc9000.txt

Cet unique bit a suscité beaucoup de discussions pour sa petite taille. Si vous voulez en apprendre d'avantage, vous pouvez consulter l'"*Internet-Draft*" `draft-andersdotter-rrm-for-rtt-in-quic` (une technique compliquée mais qui contient une bonne explication du "*spin bit*"), ou bien le `draft-martini-hrpc-` qui, globalement, était très enthousiaste en faveur de QUIC mais suggèrait la suppression du "*spin bit*". Merci d'ailleurs à leurs auteurs, pour leurs explications qui m'ont beaucoup aidé. Il y a également l'article « "*Three Bits Suffice : Explicit Support for Passive Measurement of Internet Latency in QUIC and TCP*" `<https://mami-project.eu/wp-content/uploads/2018/09/spinbit.pdf>` » (la version finale du "*spin bit*" est différente mais l'article explique bien le principe).

`https://www.bortzmeyer.org/quic-spin-bit.html`