RFC 8740 : Using TLS 1.3 with HTTP/2

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 24 février 2020

Date de publication du RFC : Février 2020

https://www.bortzmeyer.org/8740.html

Voici un très court RFC, pour résoudre un petit problème d'interaction entre TLS 1.3 et HTTP/2. (Mais ne le lisez pas, il a depuis été intégré au RFC 9113[1].)

Les anciennes versions du protocole de sécurité TLS avaient un mécanisme de renégociation des paramètres de la session, permettant de changer certains paramètres même après que la session ait démarré. C'était parfois utilisé pour l'authentification du client TLS, par exempe lorsqu'un serveur HTTP décide de demander ou pas un certificat client en fonction de la requête dudit client. Or, dans la version 2 de HTTP, HTTP/2, normalisée à l'origine dans le RFC 7540, il peut y avoir plusieurs requêtes HTTP en parallèle. On ne peut donc plus corréler une requête HTTP avec une demande de certificat. Le RFC 7540 (section 9.2.1) interdit donc d'utiliser la renégociation.

Mais la nouvelle version de TLS, la 1.3, spécifiée dans le RFC 8446, a supprimé complètement le mécanisme de renégociation. À la place, un mécanisme d'authentification spécifique a été normalisé (section 4.6.2 du RFC 8446.) Or, ce mécanisme pose les mêmes problèmes que la rénégociation avec le parallélisme que permet HTTP/2. Il fallait donc l'exclure aussi, ce qui n'avait pas été remarqué tout de suite. C'est ce que fait notre RFC. Pas d'authentification après la poignée de main initiale, elle est incompatible avec HTTP/2 (ou avec le futur HTTP/3, d'ailleurs, qui permet également des requêtes en parallèle) et elle doit déclencher une erreur.

À noter que la renégociation était également utilisée pour dissimuler le vrai certificat serveur, par exemple pour contourner certaines solutions de censure. Comme TLS 1.3 chiffre désormais le certificat serveur, la renégociation n'est plus utile pour ce scénario. En outre, la renégociation avait posé quelques problèmes de sécurité (cf. une faille fameuse <https://www.bortzmeyer.org/tls-renego.html>, et le RFC 7457.)

Outre la renégociation, il y a d'autres messages qui peuvent survenir après la poignée de main initiale. C'est le cas des `KeyUpdate` (RFC 8446, sections 4.6.3 et 7.2) mais ils concernent la session TLS entière, pas juste une requête HTTP, donc ils sont compatibles avec le parallélisme de HTTP/2. Quant aux `NewSessionTicket` (RFC 8446, section 4.6.1), ils dépendent, eux, de la requête HTTP, mais leur interaction avec HTTP/2 est prévue et documentée dans le RFC 8470, et ils sont donc acceptés. De toute façon, depuis, le problème a été réglé par le remplacement du RFC 7540 par le RFC 9113.

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc9113.txt