RFC 9150 : TLS 1.3 Authentication and Integrity-Only Cipher Suites

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 22 avril 2022

Date de publication du RFC : Avril 2022

https://www.bortzmeyer.org/9150.html

Ce nouveau RFC normalise des algorithmes pour le protocole de sécurité TLS, qui ne fournissent **pas** de chiffrement (seulement authentification et intégrité). C'est évidemment une option très contestée et l'IETF ne suggère pas d'utiliser ces algorithmes mais, bon, certaines personnes y voient une utilité.

La section 1 du RFC décrit des scénarios d'usage (souvent tirés du monde de l'IoT) où cela peut avoir un sens de ne pas chiffrer. Le premier exemple est celui d'un bras robotique commandé via un protocole TCP/IP. L'authentification est importante mais la confidentialité ne l'est peut-être pas, ce qui rendrait acceptable l'absence de chiffrement. Autre exemple, des rapports météo, ou bien l'envoi de signaux d'horloges, qu'il faut évidemment authentifier mais qui ne sont pas secrets. Le RFC cite aussi des exemples de communication avec des trains ou des avions, où l'intégrité des données est cruciale, mais pas leur confidentialité. Mais attention avant de jeter le chiffrement à la poubelle, le RFC dit bien qu'il faut faire une analyse soignée de la menace. Pour reprendre l'exemple du bras robotique, l'écoute des messages pourrait permettre la rétro-ingénierie, ce qu'on ne souhaite pas forcément.

Mais pourquoi se passer de chiffrement, d'ailleurs, alors qu'il est plus simple de l'utiliser systématiquement ? Parce que dans certains cas, il coûte cher, notamment en latence <https://www.bortzmeyer.org/latence.html>. En outre, certains équipements, notamment du genre objets connectés, ont des capacités de calcul très limitées. Bref, si le chiffrement systématique et par défaut reste la politique de l'IETF, ce RFC présente quelques façons de s'en passer, **si on sait ce qu'on fait** (si vous ne savez pas, continuez à chiffrer !).

Les algorithmes sans chiffrement sont présentés dans la section 4. Ils se nomment `TLS_SHA256_SHA256` et `TLS_SHA384_SHA384`, et sont évidemment dans le registre IANA <https://www.iana.org/assignments/tls-parameters/tls-parameters.xml#tls-parameters-4>. Ils utilisent une fonction de condensation comme SHA-256 pour faire du HMAC, protégeant ainsi l'intégrité des communications.

Rappelez-vous bien : aucun chiffrement n'est fourni. Les certificats client, par exemple, qui sont normalement chiffrés depuis TLS 1.3, seront envoyés en clair.

Publier un tel RFC n'a pas été facile, la crainte de beaucoup étant que des gens qui ne comprennent pas bien les conséquences utilise ces algorithmes sans mesurer les risques. Le RFC demande (section 9) donc qu'ils ne soient pas utilisés par défaut et qu'ils requièrent une configuration explicite. Et rappelez-vous que ce RFC n'est que « pour information » et ne fait pas l'objet d'un consensus à l'IETF.