RFC 8143 : Using Transport Layer Security (TLS) with Network News Transfer Protocol (NNTP)

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 25 avril 2017

Date de publication du RFC : Avril 2017

http://www.bortzmeyer.org/8143.html

Ce RFC concernant le protocole NNTP met à jour l'ancien RFC 4642 [1] qui donnait des conseils TLS très spécifiques (activer la compression, utiliser RC4...), conseils qui n'ont pas résisté à l'évolution de la cryptographie. On arrête donc de donner des conseils TLS spécifiques, NNTP a un usage générique de TLS et doit donc se référer au RFC générique BCP 195 <https://www.rfc-editor.org/info/bcp195> (actuellement RFC 7525).

NNTP, le protocole de transport des News, est normalisé dans le RFC 3977. Il peut utiliser TLS (RFC 5246) pour sécuriser la communication entre deux serveurs NNTP, ou bien entre serveur et client. Le RFC 4642, qui décrivait cet usage de TLS, faisait une erreur : il donnait des conseils de cryptographie. Or, d'une part, NNTP ne faisait pas un usage particulier de la cryptographie, et n'avait pas besoin de recommandations spécifiques et, d'autre part, la cryptographie est un domaine qui évolue. Ainsi, les fonctions de compression de données de TLS sont aujourd'hui considérées comme une mauvaise idée, dans la plupart des cas (attaque CRIME, cf. RFC 7525, section 3.3).

L'essentiel de notre nouveau RFC est dans sa section 3 : désormais, il faut suivre le RFC de bonnes pratiques TLS, BCP 195 <https://www.rfc-editor.org/info/bcp195> (actuellement RFC 7525).

De même que le courrier électronique peut préciser dans un en-tête `Received:` que la connexion SMTP était protégée par TLS, de même NNTP permet d'ajouter dans le champ `Path:` (section 3.1.5 du RFC 5536) une indication que le pair a été authentifié (deux points d'exclamation de suite).

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc4642.txt

La section 2 du RFC résume les changements par rapport au RFC 4642 (la liste complète est dans l'annexe A). Comme dit plus haut, la compression TLS est désormais fortement déconseillée (à la place, on peut utiliser l'extension de compression de NNTP, normalisée dans le RFC 8054). Il est très nettement recommandé d'utiliser du TLS implicite (connexion sur un port dédié (le 563 pour les clients, non spécifié pour les autres serveurs), au lieu de la directive `STARTTLS`, qui est vulnérable à l'attaque décrite dans la section 2.1 du RFC 7457). Il ne faut évidemment plus utiliser RC4 (cf. RFC 7465), mais les algorithmes de chiffrement obligatoires de TLS. Il faut utiliser l'extension TLS "*Server Name Indication*" (RFC 6066, section 3). Et, pour authentifier, il faut suivre les bonnes pratiques TLS des RFC 5280 et RFC 6125.

Comme la plupart des mises en oœuvre de NNTP-sur-TLS utilisent une bibliothèque TLS générique, elles suivent déjà une bonne partie des recommandations de ce RFC. Après, tout dépend des options particulières qu'elles appellent…

Merci à Julien Élie pour une relecture attentive (j'avais réussi à mettre plusieurs erreurs dans un article aussi court.)