Thunderbird et la cryptographie, des options pas toujours évidentes

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 6 décembre 2008

https://www.bortzmeyer.org/thunderbird-et-crypto.html

Le MUA Thunderbird permet d'utiliser la cryptographie pour protéger le relevé ou l'envoi du courrier. Mais trouver la bonne option n'est pas facile !

Une fois des serveurs de messagerie configurés pour utiliser le protocole de cryptographie TLS (pour Postfix, voir « Configurer Postfix avec TLS <https://www.bortzmeyer.org/postfix-tls.html> »), il reste à configurer les clients.

Thunderbird est un des plus utilisés. Logiciel libre, à interface graphique, il dispose de nombreuses fonctions, notamment de filtrage des spams par algorithme bayésien. Il dispose également du protocole TLS. Mais il n'est pas évident de choisir l'option à activer, notamment en raison d'un nommage bizarre des protocoles.

Sans "*Secure connections - Thunderbird*" <http://kb.mozillazine.org/Secure_connections_-_Thunderbird>, je ne serai jamais arrivé à le configurer en mode « 100 % crypto » (pour IMAP et SMTP). Cela relativise l'argument comme quoi les interfaces graphiques sont forcément simples. Le problème est qu'il est trivial de trouver quoi faire pour activer "TLS" (on clique sur un bouton) mais moins évident de savoir s'il faut choisir "TLS", "TLS, if available" ou "SSL". SSL et TLS sont pourtant la même chose (SSL est l'ancien nom du protocole qui est devenu TLS et est aujourd'hui normalisé dans le RFC 5246 [1]).

Les options "TLS" et "TLS, "*if available*"" font presque la même chose, et qui est en fait du STARTTLS (commencer en clair puis basculer en chiffré s'il est disponible). La seule différence est que "TLS" tout court impose que STARTTLS soit possible et coupe la communication si cette sécurité n'est pas posisble.

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc5246.txt

C'est l'option "SSL", très mal nommée, qui permet de faire du TLS directement (sans STARTTLS).

Donc, en SMTP : il faut configurer "TLS" (qui veut dire en fait STARTTLS) et le port 587, le port de soumission du courrier (RFC 6409).

En IMAP, avec la configuration par défaut du serveur IMAP Courier (deux ports, un pour le clair et un pour le chiffré), il faut "SSL" et ne pas cocher ""*secure authentication*"" (qui désigne un défi/réponse, mais c'est déjà assez sûr avec TLS) et il **faut** un certificat correct, le certificat auto-signé généré par Courier par défaut ne marche pas (mais le certificat de ma CA privée fonctionne).

(Courier peut aussi être configuré pour faire du STARTTLS dans IMAP.)

Merci à Erwan David pour ses explications.