RFC 5425 : TLS Transport Mapping for Syslog

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 10 mars 2009

Date de publication du RFC : Mars 2009

https://www.bortzmeyer.org/5425.html

Le protocole syslog, de transport des données de journalisation entre deux machines TCP/IP, a toujours souffert de son absence de sécurité. Ce RFC normalise un transport des données authentifié et chiffré, grâce au protocole TLS, et permet donc de combler une des failles de sécurité de syslog.

Les sections 8.5, 8.7 et 8.8 du RFC 5424 [1] et la section 2 de notre RFC 5425 notent bien que de nombreuses attaques sont possibles contre le syslog traditionnel. Notamment, deux nous intéressent particulièrempent ici :

— La possibilité d'écouter les données, souvent sensibles, qui circulent sur le réseau,
— La possibilité pour un tiers d'intercepter des données à la place du vrai récepteur.

Il faut aussi se rappeler qu'un message syslog peut être **relayé** par des machines intermédiaires, augmentant ainsi les risques. TLS (RFC 5246) traite ces deux problèmes pour bien d'autres protocoles. Il utilise la cryptographie pour protéger les communications des indiscrets et des usurpateurs. Son utilisation pour syslog allait donc de soi.

La section 2 expose par contre que certains risques ne sont pas pris en compte, par exemple celui de déni de service. TLS augmente plutôt ce risque, en exigeant davantage de ressources disponibles de la part des deux machines. (Le transport UDP du RFC 5426 est plus léger mais bien moins sûr.) La section 3 fait remarquer que l'usage de TLS ne protège pas non plus contre un faux message : si on veut signer ses messages syslog, il faut utiliser un autre mécanisme, actuellement en cours de développement.

Enfin, la section 4 décrit en détail le protocole. Il utilise le port 6514. Il se sert des certificats du RFC 5280 pour l'authentification de l'autre machine (sections 4.2 et 5, la seconde sur les politiques d'authentification). Les données sont ensuite simplement encapsulées dans TLS (section 4.3).

Je ne connais pas encore de mise en œuvre du protocole syslog qui aie ce transport sécurisé.

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc5424.txt