RFC 9109 : Network Time Protocol Version 4: Port Randomization

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 13 septembre 2021

Date de publication du RFC : Août 2021

https://www.bortzmeyer.org/9109.html

Le protocole NTP utilisait traditionnellement un port bien connu, 123, comme source et comme destination. Cela facilite certaines attaques en aveugle, lorsque l'attaquant ne peut pas regarder le trafic, mais sait au moins quels ports seront utilisés. Pour compliquer ces attaques, ce RFC demande que NTP utilise des numéros de ports aléatoires autant que possible.

NTP est un très vieux protocole (sa norme actuelle est le RFC 5905[1] mais sa première version date de 1985, dans le RFC 958). Dans son histoire, il a eu sa dose des failles de sécurité <http://support.ntp.org/bin/view/Main/SecurityNotice>. Certaines des attaques ne nécessitaient pas d'être le chemin entre deux machines qui communiquent car elles pouvaient se faire en aveugle. Pour une telle attaque, il faut deviner un certain nombre de choses sur la communication, afin que les paquets de l'attaquant soient acceptés. Typiquement, il faut connaitre les adresses IP source et destination, ainsi que les ports source et destination et le "*key ID*" de NTP (RFC 5905, section 9.1). NTP a plusieurs modes de fonctionnement (RFC 5905, sections 2 et 3). Certains nécessitent d'accepter des paquets non sollicités et, dans ce cas, il faut bien écouter sur un port bien connu, en l'occurrence 123. Mais ce n'est pas nécessaire dans tous les cas et notre RFC demande donc qu'on n'utilise le port bien connu que si c'est nécessaire, au lieu de le faire systématiquement comme c'était le cas au début de NTP et comme cela se fait encore trop souvent (« "*Usage Analysis of the NIST Internet Time Service*" <https://tf.nist.gov/general/pdf/2818.pdf> »). C'est une application à NTP d'un principe général sur l'Internet, documenté dans le RFC 6056 : n'utilisez pas de numéros de port statiques ou prévisibles. Si on suit ce conseil, un attaquant en aveugle aura une information de plus à deviner, ce qui gênera sa tâche. Le fait d'utiliser un port source fixe a valu à NTP un CVE, CVE-2019-11331 <https://nvd.nist.gov/vuln/detail/CVE-2019-11331>.

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc5905.txt

La section 3 du RFC résume les considérations à prendre en compte. L'idée de choisir aléatoirement le port source pour faire face aux attaques en aveugle est présente dans bien d'autres RFC comme le RFC 5927 ou le RFC 4953. Elle est recommandée par le RFC 6056. Un inconvénient possible (mais mineur) est que la sélection du chemin en cas d'ECMP peut dépendre du port source (calcul d'un condensat sur le tuple à cinq élements {protocole, adresse IP source, adresse IP destination, port source, port destination}, avant d'utiliser ce condendat pour choisir le chemin) et donc cela peut affecter les temps de réponse, troublant ainsi NTP <http://leapsecond.com/ntp/NTP_Paper_Sommars_PTTI2017.pdf>, qui compte sur une certaine stabilité du RTT. D'autre part, le port source aléatoire peut gêner certaines stratégies de filtrage par les pare-feux : on ne peut plus reconnaitre un client NTP à son port source. Par contre, un avantage du port source aléatoire est que certains routeurs NAT sont suffisamment bogués pour ne pas traduire le port source s'il fait partie des ports « système » (inférieurs à 1 024), empêchant ainsi les clients NTP situés derrière ces routeurs de fonctionner. Le port source aléatoire résout le problème.

Assez de considérations, passons à la norme. Le RFC 5905, section 9.1, est modifié pour remplacer la supposition qui était faite d'un port source fixe par la recommandation d'un port source aléatoire.

Cela ne pose pas de problème particulier de mise en œuvre. Par exemple, sur un système POSIX, ne **pas** faire de `bind()` sur la prise suffira à ce que les paquets associés soient émis avec un port source aléatoirement sélectionné par le système d'exploitation.

À propos de mise en œuvre, où en sont les logiciels actuels ? OpenNTPD <https://www.openntpd.org> n'a jamais utilisé le port source 123 et est donc déjà compatible avec la nouvelle règle. Même chose pour Chrony <https://chrony.tuxfamily.org/>. Par contre, à ma connaissance, ntpd <http://www.ntp.org/> ne suit pas encore la nouvelle règle.