La sécurité de TCP : plein de nouveaux RFC depuis trois ans

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 28 octobre 2010

https://www.bortzmeyer.org/tcp-security.html

Le protocole de transport TCP, normalisé dans le RFC 793 [1] il y a presque trente ans, est le cheval de labour numéro 1 de l'Internet. Malgré l'utilisation intensive d'UDP pour certains transferts de vidéo, malgré la présence de concurrents plus récents, plus perfectionnés, mais nettement moins utilisés, comme SCTP, la grande majorité des octets de données qui voyagent sur l'Internet le font dans un paquet TCP. Mais TCP n'est pas un modèle de sécurité. Tel qu'il était mis en œuvre à l'origine, il était trop facile à tromper, on pouvait couper une connexion, voire injecter de fausses données. Petit à petit, ces failles ont été comblées, notamment par l'excellent travail du groupe IETF tcpm <http://tools.ietf.org/wg/tcpm> ("*TCP Maintenance and Minor Extensions*"). Ce court article résume les principaux RFC sur la sécurité de TCP.

Le premier a sans doute été le RFC 4953 qui exposait le principe des attaques par fabrication de faux paquets TCP et donnait quelques pistes de solutions. Des protocoles de sécurité au niveau applicatif comme SSH (RFC 4251) ne résolvent pas ces problèmes : la connexion TCP sous-jacente peut toujours être ralentie ou coupée par de faux paquets. Il fallait donc des solutions au niveau de TCP.

Ensuite, le RFC 5927, en juillet 2010, se focalisait sur les attaques utilisant ICMP, avec des paquets de contrôle prétendant être lié à une connexion TCP (ces attaques ICMP contre TCP avaient été découvertes par Fernando Gont <http://www.gont.com.ar/tools/icmp-attacks/index.html> en 2005). Il fournit sur son site un outil complet pour les exploiter. Le RFC 5927 appelle les programmeurs de TCP à accepter avec plus de prudence les paquets ICMP.

Certaines attaques peuvent se faire entièrement par TCP, comme les attaques RST, documentées dans le RFC 5961, en août 2010, ainsi que les solutions proposées (là encore, accepter les paquets entrants avec moins de confiance, et notamment vérifier les numéros de séquence).

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc793.txt

Enfin, le RFC 6056 sur l'aléatoirisation des numéros de port. Son idée est de compliquer la tâche des attaquants aveugles, en rendant peu prévisible l'un des éléments qui permettent l'identification d'un paquet TCP, le numéro de port. Cette sécurité est déjà mise en œuvre dans tous les Unix libres (à l'exception de NetBSD).

Certes, toutes les attaques décrites ici pourraient être évitées en généralisant l'usage d'IPsec (RFC 4301). Mais ce protocole de sécurité, bien trop complexe, pas toujours présent dans les implémentations, celles-ci étant par ailleurs mal documentées, reste peu utilisé. D'où l'idée de solutions moins générales mais qui peuvent apporter un réel progrès de sécurité à TCP, comme l'option d'authentification du RFC 5925. On peut noter que, contrairement aux solutions indiquées plus haut (contrôle de la vraisemblance des numéros de séquence, choix d'un port non prévisible), l'option d'authentification fonctionne non seulement contre l'attaquant aveugle, qui ne peut pas "*sniffer*" le réseau, mais aussi contre celui qui peut regarder à loisir les paquets qui passent.

Un bon article expliquant de manière très pédagogique les problèmes de sécurité de TCP (mais, très ancien, il ne contient pas grand'chose sur les solutions) est « "*TCP/IP Security*" <http://www.linuxsecurity.com/resource_files/documentation/tcpip-security.html> de Chris Chambers, Justin Dolske, et Jayaraman Iyer.