RFC 8558 : Transport Protocol Path Signals

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 6 juin 2019

Date de publication du RFC : Avril 2019

https://www.bortzmeyer.org/8558.html

Ce nouveau RFC de l'IAB examine les **signaux** envoyés par un protocole de transport aux couches supérieures. Par exemple, la machine à états de TCP est observable de l'extérieur, on peut déduire son état de l'examen des paquets envoyés. Certains de ces signaux sont **explicites**, prévus pour être lus par les routeurs, d'autres sont **implicites**, déduits de certains comportements. Le RFC recommande de compter plutôt sur les signaux explicites, documentés et fiables. Attention, la tendance actuelle est, pour protéger la vie privée et pour limiter les interférences du réseau avec les communications, de limiter les signaux envoyés. Ainsi, QUIC <https://www.bortzmeyer.org/quic.html> envoie nettement moins de signaux que TCP.

Le principe de bout en bout dit que les éléments du réseau ne devraient pas avoir besoin de ces signaux du tout (RFC 1958 [1]). Ils devraient transporter les datagrammes, point. Mais en pratique, des raisons plus ou moins légitimes font que des équipements intermédiaires ont besoin d'accéder à des informations sur le transport. C'est par exemple le cas des routeurs NAT (RFC 3234).

Comme exemple de signaux implicites, on peut citer ceux de TCP (RFC 793). Les messages échangés (SYN, RST, FIN...) sont destinés aux extrémités, pas aux boitiers intermédiaires mais, comme ils sont visibles (sauf utilisation d'IPsec), le réseau peut être tenté de s'en servir comme signaux implicites. C'est ce que fait un pare-feu à état quand il utilise ces messages pour déterminer si la connexion a été demandée depuis l'intérieur (auquel cas elle est souvent autorisée) ou de l'extérieur (auquel cas elle est souvent interdite).

Cette observation des signaux implicites a souvent pour but une action (blocage des connexions entrantes, dans l'exemple ci-dessus, ou bien déni de service en envoyant des faux RST). Il est donc logique que les protocoles cherchent à se protéger en chiffrant la communication. TLS ou SSH ne chiffrent que l'application, et restent donc vulnérables aux attaques visant la couche 4. D'où le développement de protocoles comme QUIC <https://www.bortzmeyer.org/quic.html>, qui chiffrent l'essentiel de la machinerie de transport.

La section 2 de notre RFC liste les signaux qui peuvent être déduits de l'observation de la couche transport en action :

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc1958.txt

— Découvrir l'établissement d'une session, et le fait que tel paquet appartienne à telle session (identifiée typiquement par un tuple {adresse IP source, adresse IP destination, protocole de transport, port source, port destination}), font partie des signaux les plus utilisés. (Pensez à l'exemple du pare-feu plus haut, ou bien à celui d'un répartiteur de charge qui veut envoyer tous les paquets d'une même session au même serveur.)
— Vérifier que la section est à double sens (les **deux** machines peuvent communiquer et le veulent) est également possible, et important. Par exemple, si le pare-feu détecte qu'une machine a initié la session, on peut supposer qu'elle veut recevoir les réponses, ce qui justifie qu'on fasse un trou dans le pare-feu pour laisser passer les paquets de cette session. (Pour le NAT, cf. RFC 7857.)
— Mesurer des caractéristiques quantitatives de la session est aussi possible. L'observation passive de TCP, par exemple, peut indiquer la latence <https://www.bortzmeyer.org/latence.html> (en mesurant le temps écoulé entre le passage des données et l'accusé de réception correspondant), ou le taux de perte de paquets (en regardant les retransmissions).

On le voit, les signaux implicites sont utilisés (pas forcément pour de bonnes raisons). Si on chiffre la couche transport, comme le fait QUIC, on perd certains de ces signaux. Que faut-il faire ? La section 3 du RFC liste, sans en recommander une particulière, plusieurs possibilités. La première est évidemment de ne rien faire. Si on chiffre, c'est justement pour assurer la confidentialité ! Le transport étant une fonction de bout en bout, les intermédiaires ne sont pas censés regarder son fonctionnement. Cette approche a quand même quelques inconvénients. Par exemple, un routeur NAT ne sait plus quand les connexions commencent et quand elles finissent, il peut donc être nécessaire d'ajouter du trafic « battement de cœur » pour maintenir l'état dans ce routeur.

On peut aussi se dire qu'on va remplacer les signaux implicites de la couche transport par des signaux explicites, conçus précisément pour une utilisation par des boitiers intermédiaires. C'est le cas du "*connection ID*" de QUIC, qui permet par exemple aux répartiteurs de charge d'envoyer tous les paquets d'une connexion QUIC donnée au même serveur. Ou du "*spin bit*" du même protocole, pour permettre certaines mesures par les intermédiaires (un bit qui a été très controversé dans la discussion à l'IETF). Le RFC note que ces signaux explicites pourraient être transportés par les en-têtes "*hop-by-hop*" d'IPv6 (RFC 7045) mais que leur capacité à être déployés sans perturber les équipements intermédiaires ne va pas de soi.

Ces signaux explicites pourraient être placés dans une mince couche intermédiaire entre UDP (qui sert de base à plusieurs protocoles de transport, comme QUIC ou comme SCTP désormais), et cette normalisation d'une couche intermédiaire avait, par exemple, été proposée dans le projet PLUS ("*Transport-Independent Path Layer State Management*" <https://datatracker.ietf.org/doc/draft-trammell-plus-st>).

Après cette étude, quelles recommandations ? La section 4 du RFC recommande évidemment que les nouveaux protocoles fournissent de la confidentialité par défaut (TCP expose trop de choses), ce qui implique le chiffrement systématique. Les signaux implicites font fuiter de l'information et devraient être évités. L'approche de QUIC est donc la bonne. Par contre, comme il peut être utile d'envoyer certaines informations aux différents équipements intermédiaires situés sur le réseau, l'IAB recommande de mettre quelques signaux explicites.

Cela nécessite de suivre les principes suivants :
— Tout ce qui est destiné aux machines terminales <https://www.bortzmeyer.org/terminal-host.html> doit être chiffré pour empêcher les "*middleboxes*" d'y accéder. Par exemple, le message de fin d'une connexion n'a pas à être public (c'est parce qu'il l'est que TCP est vulnérable aux attaques avec des faux RST).
— Les signaux explicites, destinés aux équipements intermédiaires, doivent être protégés. Que le réseau puisse les lire, d'accord, mais il n'y a aucune raison qu'il puisse les modifier.
— Les signaux explicites doivent être séparés des informations et messages destinés aux machines terminales.

— Les machines intermédiaires ne doivent pas ajouter de signaux (le RFC cite le RFC 8164 mais je trouve le RFC 8165 plus pertinent). Les machines terminales ont intérêt à protéger l'intégrité du paquet, pour éviter ces ajouts.

Notez que cette intégrité ne peut être vérifiée que par les machines terminales, les machines du réseau n'ayant pas le matériau cryptographique (les clés) nécessaires.

Reste enfin les questions de sécurité (section 6 du RFC). Le modèle de menace classique sur l'Internet est qu'on ne peut pas faire confiance aux intermédiaires : sur le trajet entre Alice et Bob, il est trop fréquent qu'au moins un des intermédiaires soit bogué, ou simplement malveillant. Tous les signaux envoyés implicitement sont dangereux, car ils peuvent donner de l'information à celui qui est peut-être un attaquant, lui facilitant certaines attaques. D'où l'importance de diminuer ces signaux implicites.

Naturellement, ce n'est pas une solution miracle ; les attaquants vont trouver d'autres méthodes et la lutte entre attaquant et défenseur ne sera donc jamais finie.

Publier des signaux explicites présente aussi des risques ; en voulant donner au réseau des informations qui peuvent lui être utiles, on peut menacer la vie privée. Ceci explique la vigueur des débats à l'IETF au sujet du "*spin bit*" <https://www.bortzmeyer.org/quic-spin-bit.html> de QUIC. Le "*spin bit*" n'a pas d'utilité pour les machines terminales, seulement pour les équipements intermédiaires. Ses partisans disaient qu'il était important que ces équipements puissent accéder à des informations sur le RTT. Ses adversaires (qui n'ont pas eu gain de cause complet, le spin bit est optionnel, on n'est pas forcé de l'envoyer) estimaient que faire fuiter volontairement de l'information, même assez inoffensive, ouvrait un risque potentiel.

Enfin, comme les signaux explicites sont déconnectés des messages échangés entre les deux machines qui communiquent, il faut se poser la question de leur authenticité. Un tiers peut les modifier pour tromper les machines suivantes sur le trajet. Les protections cryptographiques ne sont pas utilisables puisqu'il n'y a aucune chance que les équipements intermédiaires disposent des clés leur permettant de vérifier ces protections. Plus drôle, si un opérateur réseau agit sur la base de ces signaux explicites, et, par exemple, favorise certaines sessions au détriment d'autres, on pourrait voir des machines terminales décider de « tricher » en envoyant délibérement de faux signaux. (Ce qui n'est pas possible avec les signaux implicites, qui sont de véritables messages, interprétés par la machine située en face.)