RFC 8811 : DDoS Open Threat Signaling (DOTS) Architecture

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 18 août 2020

Date de publication du RFC : Août 2020

https://www.bortzmeyer.org/8811.html

Ce nouveau RFC décrit l'architecture du système DOTS ("*Distributed-Denial-of-Service Open Threat Signaling*"), un ensemble de mécanismes pour permettre aux victimes d'attaques par déni de service de se coordonner avec les fournisseurs de solution d'atténuation. C'est juste l'architecture, les protocoles concrets sont dans d'autres RFC, comme le RFC 9132 [1].

Il n'y a pas besoin d'expliquer que les attaques par déni de service sont une plaie. Tout le monde en a déjà vécu. Une des approches pour atténuer l'effet d'une de ces attaques est de sous-traiter votre trafic à un tiers, l'atténuateur (« Victor, atténuateur ») qui va recevoir les données, les classer, et jeter ce qui est envoyé par l'attaquant. Cette approche nécessite de la communication entre la victime et l'atténuateur, communication qui se fait actuellement de manière informelle (téléphone…) ou via des protocoles privés. L'idée de DOTS ("*Distributed-Denial-of-Service Open Threat Signaling*") est d'avoir des protocoles normalisés pour ces fonctions de communication. Les scénarios typiques d'utilisation de DOTS sont décrits dans le RFC 8903.

Dans le cas le plus fréquent, DOTS sera utilisé entre des organisations différentes (la victime, et le fournisseur de solutions anti-dDoS). A priori, ils auront une relation contractuelle (du genre contrat, et paiement) mais cette question ne fait pas l'objet du RFC, qui mentionne seulement l'architecture technique. Mais en tout cas, ce caractère multi-organisations va nécessiter des mécanismes d'authentification sérieux (le cahier des charges complet de DOTS est le RFC 8612).

La section 1 de notre RFC rappelle également que DOTS, par définition, sera utilisé dans des moments difficiles, pendant une attaque (RFC 4732), et qu'il est donc conçu en pensant à des cas où les ressources sont insuffisantes (les paquets ont du mal à passer, par exemple). Parfois, il y aura un lien

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc9132.txt

intact entre le client DOTS et le serveur, ou bien un réseau dédié pour cette communication, ou encore une qualité de service garantie pour les échanges DOTS, mais on ne pourra pas toujours compter dessus. DOTS doit fonctionner sur l'Internet normal, possiblement affecté par l'attaque. C'est un élément à systématiquement garder en tête lorsqu'on examine le protocole DOTS, et qui explique bien des choix, comme UDP pour le protocole de signalisation du RFC 9132.

D'autre part, les RFC sur DOTS décrivent des techniques, pas des politiques. Comment on définit une attaque DoS, à partir de quand on déclenche l'atténuation, comment on choisit un atténuateur, toutes ces questions dépendent de la victime, chacun peut faire des choix différents.

Ceci étant posé, place à la description de haut niveau de DOTS, en section 2. Dans le cas le plus simple il y a :

- La victime, qui héberge un client DOTS,
- L'atténuateur qui héberge un serveur DOTS.

Et client et serveur DOTS communiquent avec les deux protocoles DOTS, celui de signalisation (RFC 9132) et celui de données (RFC 8783). Il y a donc **deux** canaux de communication. DOTS permet également des schémas plus complexes, par exemple avec plusieurs serveurs, à qui le client demande des choses différentes, ou bien avec des serveurs différents pour la signalisation et pour les données. Notez bien que DOTS est uniquement un protocole de communication entre la victime et l'atténuateur qui va essayer de la protéger. Comment est-ce que l'atténuateur filtre, ou comment est-ce qu'on lui envoie le trafic à protéger, n'est pas normalisé. De même, DOTS ne spécifie pas comment le serveur répond aux demandes du client. Le serveur peut refuser d'aider, par exemple parce que le client n'a pas payé. (Pour l'envoi du trafic à protéger, il y a deux grandes techniques, fondées sur BGP ou sur DNS. Le trafic une fois filtré est ensuite renvoyé à la victime. Une autre solution est d'avoir le mitigateur dans le chemin en permanence.)

On a vu qu'il y avait deux canaux de communication. Celui de signalisation, normalisé dans le RFC 9132 sert surtout à demander à l'atténuateur une action de protection, et à voir quelles réponses l'atténuateur donne. C'est ce canal qui devra fonctionner au plus fort de l'attaque, ce qui lui impose des contraintes et des solutions particulières. Le canal de données, spécifié dans le RFC 8783, n'est pas en toute rigueur indispensable à DOTS, mais il est quand même pratique : il sert à envoyer des informations de configuration, permettant au client de spécifier plus précisement ce qu'il veut protéger et contre qui. Par exemple, il va permettre de donner des noms à des ressources (une ressource peut être, par exemple, un ensemble de préfixes IP), envoyer une liste noire d'adresses d'attaquants à bloquer inconditionnellement, une liste blanche de partenaires à ne surtout pas bloquer, à définir des ACL, etc. En général, ce canal de données s'utilise avant l'attaque, et utilise des protocoles habituels, puisqu'il n'aura pas à fonctionner pendant la crise.

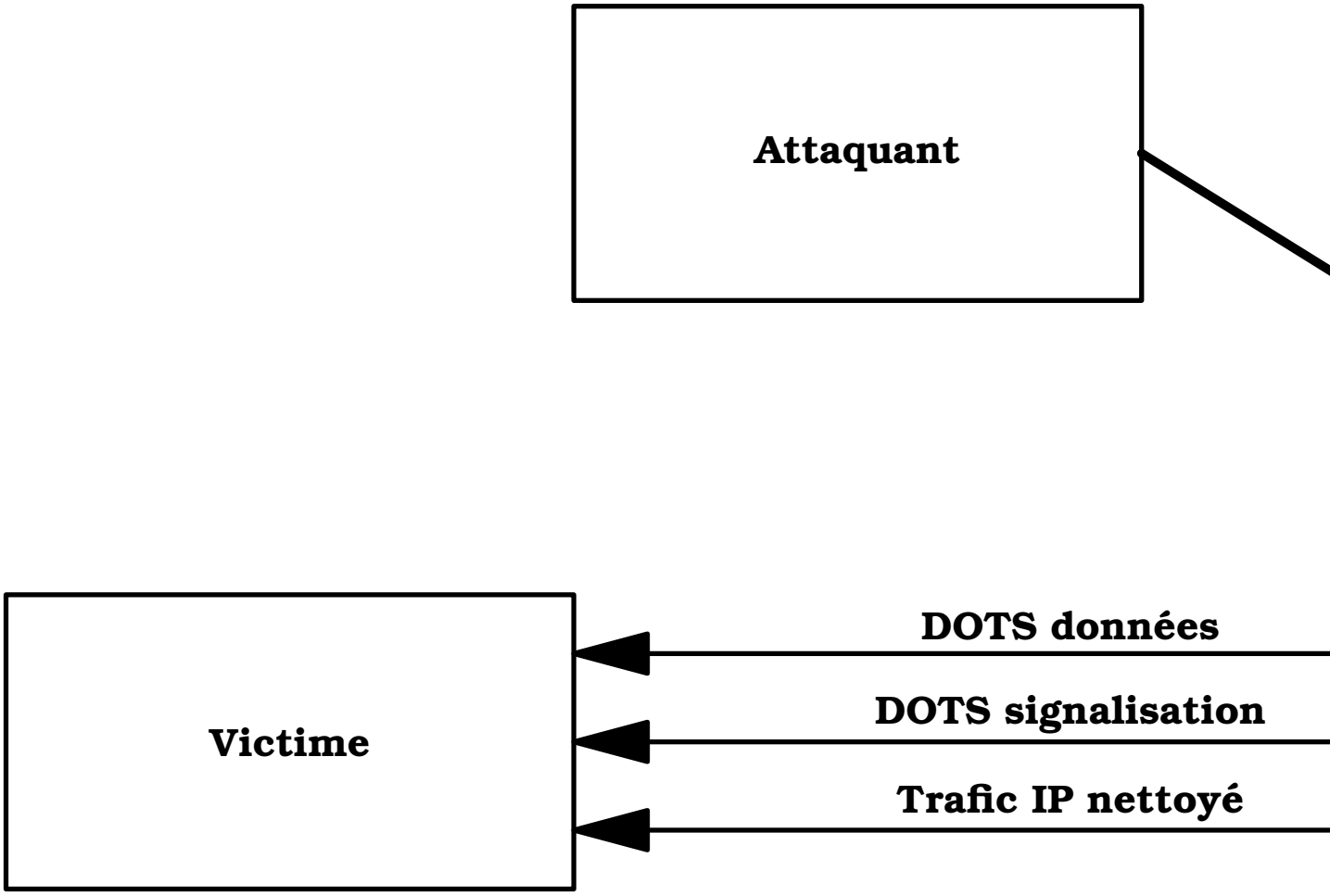
Le RFC note aussi que DOTS n'a de sens qu'entre partenaires qui ont une relation pré-existante (par exemple client / fournisseur payant). Il n'y a pas de serveur DOTS public. L'authentification réciproque du client et du serveur est donc nécessaire, d'autant plus qu'on utilise DOTS pour faire face à des attaques et que l'attaquant peut donc chercher à subvertir DOTS.

Le serveur DOTS doit non seulement authentifier le client mais aussi l'autoriser à demander une mitigation pour telle ou telle ressource (préfixe IP ou nom de domaine). Par exemple, le serveur DOTS peut utiliser les IRR pour déterminer si son client est vraiment légitime pour demander une intervention sur telle ressource. Mais il pourrait aussi utiliser ACME (RFC 8738).

Typiquement, le client établit une session de signalisation avec le serveur, qu'il va garder pendant l'attaque. Il n'y a pas actuellement de norme sur comment le client trouve le serveur DOTS. On peut supposer qu'une fois l'accord avec le serveur fait, le gérant du serveur communique au client le nom ou l'adresse du serveur à utiliser.

La section 3 du RFC détaille certains points utiles. À lire si vous voulez comprendre toute l'architecture de DOTS, notamment les configurations plus complexes, que j'ai omises ici.

Et si vous vous intéressez aux mises en œuvre de DOTS, elles sont citées à la fin de mon article sur le RFC 9132.


Attaquant
Victime
DOTS données
DOTS signalisation
Trafic IP nettoyé