Sécurité du pair-à-pair et composant central

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 16 mars 2013

https://www.bortzmeyer.org/pairapair-securite.html

Les techniques fondées sur le pair-à-pair sont souvent présentées comme permettant un Internet sans centre et sans autorité. Ce n'est vrai que si on ne se préoccupe pas de sécurité. Dès qu'on est confronté à des méchants qui tentent délibérement d'attaquer le réseau, le problème est bien plus complexe. Désolé de jouer les porteurs de mauvaise nouvelle mais la plupart des promoteurs du pair-à-pair se font des illusions.

Quel est le problème ? Les participants à un réseau pair-à-pair doivent accomplir un certain nombre d'actions pour que le réseau fonctionne. Par exemple, dans une DHT, ils doivent faire suivre les requêtes qui ne sont pas pour eux, ils doivent stocker les données qui sont pour eux, et ils doivent les restituer lorsque c'est demandé. Un nœud byzantin dans une DHT et plus rien ne marche. De même, dans un réseau maillé pair-à-pair, chacun doit faire suivre les messages, pas les garder et pas les modifier (dans les réseaux classiques, les opérateurs ne se gênent pas pour tripoter les messages <http://reflets.info/sfr-modifie-le-source-html-des-pages-que-vous-visitez-en-3g/> de leurs clients).

Bon, pas de problème, disent les défenseurs du pair-à-pair, il suffit d'avoir de la redondance. Dans une DHT, on va confier chaque donnée à N pairs et pas à un seul. Un seul méchant ne pourra donc pas bloquer le fonctionnement de la DHT. Même chose pour le réseau maillé : s'il y a plusieurs chemins possibles entre deux pairs, un seul méchant ne pourra pas empêcher la communication.

Mais ce mécanisme ne marche que si les attaquants sont nettement moins nombreux que les défenseurs. Bruce Schneier a écrit beaucoup de textes intéressants à ce sujet. Dans une société normale, les gens honnêtes sont plus nombreux que les délinquants et pas mal de mécanismes de sécurité du monde réel fonctionnent sur cette base. Mais ce modèle ne peut pas se transmettre aux réseaux informatiques : ici, l'attaquant peut générer autant d'identités qu'il le veut. Cela se nomme une attaque Sybil. Dans une DHT de 10 000 pairs, l'attaquant crée 20 000 machines virtuelles, elles rejoignent la DHT et peuvent la bloquer complètement. « Bourrer les urnes » est trivial dans le monde virtuel.

La clé de la sécurité d'un tel réseau pair-à-pair est le mécanisme d'**inscription** des pairs ("*enrollment*", dans la langue de Will Smith). Dans les réseaux complètement "*open bar*", tout pair qui arrive est pris, immédiatement. Dans d'autres, il y a un processus de vérification : authentification et autorisation du

pair. Et qui va la faire, cette vérification ? Elle ne peut pas être faite par les autres pairs (ou bien on retombe dans le problème précédent). Elle est donc forcément faite par un composant **central** (ou, à la rigueur, par un système hiérarchique, avec délégation de l'autorité). Celui-ci va alors dire « OK, tu a un certificat valide, tu es inscrit » ou bien « non, rejeté ». Cela marche, mais il a fallu accepter de ne pas faire du pair-à-pair pur.

Tous les systèmes de pair-à-pair qui fonctionnnent ont un tel composant central. Parfois, toutes les machines sont dans la même entreprise (l'inscription est alors un problème simple). Parfois, ce n'est pas le cas, mais tous les pairs font confiance à un système d'inscription central. Les systèmes qui n'ont pas un tel composant central d'inscription (comme le réseau maillé Qaul <http://qaul.net> qui se prétend utilisable dans un environnement hostile) s'écrouleront à la première attaque.

Cette impossibilité d'empêcher les attaques Sybil sans composant central (ou hiérarchique) est-elle prouvée mathématiquement (comme on a prouvé le théorème CAP) ? À ma connaissance, non. Il y a donc un espoir pour les chercheurs mais n'espérez pas trop : le problème est **difficile**.

Et BitTorrent, me dira t-on ? Les pairs utilisant une DHT ("*trackerless*") récupèrent tous les jours leurs fichiers (d'ailleurs, si quelqu'un a la saison 3 de "*Game of Thrones*", ça m'intéresse) et sans composant central. Mais si ! Le composant central est le moteur de recherche (par exemple The Pirate Bay) qui distribue les sommes de contrôle grâce auquel on vérifie qu'on a bien récupéré le fichier voulu. De même, si on veut juste stocker des données dans une DHT et vérifier qu'elles n'ont pas été modifiées par les pairs stockeurs, il existe des méthodes <https://www.bortzmeyer.org/authenticite-dans-dht.html> mais elles nécessitent d'avoir obtenu la clé de manière sécurisée, donc typiquement par un composant central.

Je résume donc mon opinion « **un réseau pair-à-pair sans composant central (ou hiérarchique) ne peut PAS être sécurisé contre les attaques Sybil** ».

Un exemple de système pair-à-pair avec inscription centralisée est le protocole RELOAD de l'IETF (RFC 6940 [1]), qui servira à faire du SIP en pair-à-pair. Le RFC 5694 est une bonne lecture, pour tous ceux et celles qui s'intéressent à la sécurité du pair-à-pair. Comme ce blog n'a pas de système de commentaires <https://www.bortzmeyer.org/no-comment.html>, si vous voulez discuter, approuver, contester, le mieux est d'aller sur SeenThis <http://seenthis.net/messages/122397>.

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc6940.txt