Attaque Sybil sur un réseau pair-à-pair

Description

L’intérêt des réseaux pair-à-pair, socle des blockchains publiques, est de se passer d’autorité centralisée pour fonctionner. Les attaques dites « Sybil » consistent à créer de fausses identités pour corrompre le réseau.

Le propre d’une architecture informatique pair-à-pair est d’opérer des échanges entre plusieurs ordinateurs connectés au système sans passer par un serveur central. Tous les ordinateurs d’un réseau pair-à-pair, appelés « nœuds », jouent tout à la fois le rôle de client et de serveur, c’est-à-dire le rôle d’émetteur et de récepteur. Une application largement répandue dans le domaine des architectures informatique pair-à-pair est celui du partage de fichiers, bête noire des industries culturelles depuis l’avènement d’internet et le lancement, en juin 1999, du premier logiciel utilisé à grande échelle, Napster, puis, à l’été 2002, du protocole de transfert de données BitTorrent. Dans le domaine des réseaux filaires ou sans fil, la structure du réseau est dite « maillée » lorsqu’elle consiste en la connexion de tous les nœuds (aussi nommés « hôtes ») en pair-à-pair, sans hiérarchie centrale. Tous les hôtes du réseau sont à la fois client et serveur, permettant une bien meilleure résilience des communications si l’un des points tombe en panne. Aujourd’hui, les réseaux pair-à-pair sont également au cœur du fonctionnement de la plupart des blockchains publiques, comme Bitcoin, Ethereum ou encore Tezos.

Toutes ces applications dont l’architecture technique repose sur un réseau pair-à-pair doivent faire face, notamment, à une menace de sécurité propre à cette topologie distribuée baptisée « attaque Sybil », au cours de laquelle une personne crée plusieurs comptes ou raccorde plusieurs nœuds ou ordinateurs au sein du réseau pour tenter d’en prendre le contrôle. Le nom de ce type d’attaque informatique est une référence à un roman biographique paru en 1973 aux États-Unis, écrit par Flora Rheta Schreiber, qui raconte l’histoire de la psychothérapie de Shirley Ardell Mason (1923-1998), également connue sous l’alias « Sybil Isabel Dorsett », une artiste publicitaire atteinte d’un trouble de la personnalité multiple, ou trouble dissociatif de l’identité. Une attaque Sybil désigne ainsi l’activité de nœuds malhonnêtes au sein d’un réseau pair-à-pair qui se font passer pour des nœuds individuels et indépendants alors qu’ils sont en réalité sous le contrôle d’une seule entité malintentionnée, et dont l’objectif est d’influencer les décisions prises sur le réseau, de « désanonymiser » les utilisateurs du réseau ou encore d’en corrompre le fonctionnement, voire d’en bloquer le protocole.

En 2014, le réseau Tor, réseau informatique mondial et décentralisé qui permet à ses utilisateurs d’anonymiser l’origine de leur connexion, a subi une attaque Sybil pendant plusieurs mois. L’objectif des attaquants, qui sont parvenus à prendre le contrôle à l’aide de nœuds malveillants d’environ la moitié des relais Tor, était d’espionner le trafic des données et de « désanonymiser » un grand nombre d’utilisateurs.

D'après Sombrecrizt, collaborateur du site linuxadictos.com, *« placer un grand nombre de nœuds contrôlés par un opérateur permet aux utilisateurs de désanonymiser à l'aide d'une attaque de classe Sybil, ce qui peut être fait si les attaquants contrôlent le premier et le dernier nœud de la chaîne d'anonymisation. Le premier nœud de la chaîne Tor connaît l'adresse IP de l'utilisateur, et ce dernier connaît l'adresse IP de la ressource demandée, qui permet de désanonymiser la demande en ajoutant une certaine étiquette cachée sur le côté du nœud d'entrée pour les en-têtes de paquets qui restent inchangés tout au long de la chaîne d'anonymisation, puis l'analyse de celui-ci côté de nœud de sortie. »* Ces nœuds malveillants, une fois identifiés, ont été déconnectés du réseau Tor.

Le risque d'attaques Sybil existe sur les protocoles blockchain dont le fonctionnement repose également sur une architecture pair-à-pair. Comment les nœuds d'une blockchain se font-ils confiance et acceptent-ils les nouveaux blocs de transactions diffusés sur le réseau ? Comment repérer d'éventuels nœuds malveillants qui tentent d'inscrire de fausses transactions à leur profit dans le registre public ? Pour se prémunir de ce type d'attaque, les blockchains publiques mettent en œuvre un mécanisme de consensus, celui notamment de la preuve de travail (*proof of work*). Le mécanisme de consensus de la preuve de travail exige que chaque nœud impliqué dans la validation des transactions résolve une énigme cryptographique, coûteuse en énergie, afin de participer au processus de minage. Celui qui résout cette énigme cryptographique valide le bloc de transactions et perçoit une récompense pour ce travail. Or, si la création d'identités multiples est toujours possible, il est aujourd'hui quasiment impossible pour un attaquant de fournir une puissance de calcul suffisante pour insérer à l'insu de tous de fausses transactions dans une blockchain publique. Le mécanisme de consensus de la preuve de travail, mis en œuvre au sein d'un protocole blockchain, permet ainsi de se défendre de manière très efficace contre les attaques Sybil. Comme le précise le site academy.binance.com, *« il n'empêche en rien un attaquant de tenter ce type d'attaque mais a pour objectif de la rendre extrêmement difficile, voire impossible »*. C'est par cet ingénieux moyen que, depuis 2009, la blockchain publique Bitcoin se prémunit avec succès contre les attaques Sybil et permet de garantir l'inviolabilité des transactions sur son réseau.

Sources :

- « Les attaques Sybil », Binance Academy, academy.binance.com/fr, 2018, mise à jour en 2021.
- « Sybil Attacks and Defenses in Internet of Things and Mobile Social Networks », Ali Alharbi, Mohamed Zohdy, Debatosh Debnath, Richard Olawoyin, George Corser, *International Journal of Computer Science Issues*, vol. 15, issue 6, zenodo.org, November 30, 2018.
- « L'attaque de Sybil – Free TON est-il vulnérable ? », Vitaly Romanov, freeton.house/fr/, 21 mars 2021.
- « Tor 11.0.2 a déjà été publié et est livré avec quelques correctifs », Sombrecrizt, linuxadictos.com/fr, 5 décembre 2021.

Categorie

1. Techniques

date créée

20 juillet 2022
Auteur
jacquesandrefines