Synthèse article PIR - ODNS = Oblivious DNS -

Aujourd'hui, presque toutes les communications sur Internet commencent avec une recherche DNS (Domain Name System). Avant de communiquer avec n'importe quelle destination Internet, un utilisateur utilise généralement d'abord un système de noms de domaine (DNS), qui prend un nom de domaine et renvoie une adresse IP pour le serveur que le client doit contacter. Aujourd'hui, le DNS demande à l'utilisateur d'accorder une grande confiance aux opérateurs DNS, qui peut voir toutes les requêtes DNS qu'il a émises.
Si l'opérateur est un fournisseur de services Internet (FAI) ou un tiers, cela est moins préoccupant que le fait qu'un seul opérateur puisse observer et conserver ces informations sensibles et confidentielles. Cet article présente un système, appelé ODNS (Oblivious DNS), qui tente de résoudre ce problème de confidentialité, côté utilisateur.

Le fonctionnement actuel du DNS aujourd'hui est tel que les requêtes et les réponses d'un utilisateur sont visibles en texte brut par un résolveur récursif, même si un canal crypté est utilisé pour la communication entre lui-même et le résolveur récursif. Ainsi, des informations telles que les noms de domaine, qui révèlent les sites Internet que les utilisateurs visitent peuvent être révélées. Dans le cas de l'IoT, les requêtes DNS actuelles peuvent renseigner les types d'appareils dans les maisons des utilisateurs. On sait aussi que les recherches DNS peuvent identifier les sites Internet visités par les utilisateurs, et ce même lorsqu'un service d'anonymisation de la navigation, tel que Tor est utilisé.
Les opérateurs de résolution DNS peuvent donc facilement associer et suivre les identités des clients (c'est-à-dire les adresses IP) ainsi que les informations à propos de leurs requêtes DNS, créant ainsi un risque pour la vie privée.

ODNS, qui signifie Oblivious DNS, est un système qui découple l'adresse IP du client (de l'utilisateur) des requêtes DNS. Cela supprime le besoin de confiance totale entre les utilisateurs et leur serveur DNS, puisqu'aucunes infrastructures DNS en dehors du réseau d'utilisateurs n'est en mesure d'obtenir les informations confidentielles qui posaient problèmes jusqu'à lors. Concrètement, cette nouvelle norme ODNS ajoute un proxy aux demandes qui se trouvent entre le client et le fournisseur DNS. Tout le trafic, et donc toutes les informations passeront en premier par ce proxy, ce qui va masquer l'adresse IP de l'utilisateur et ainsi ajouter une couche de confidentialité supplémentaire. Le serveur DNS communique également avec ce proxy et non directement avec le client. Le serveur DNS verra donc seulement l'adresse IP du proxy, et plus celle de l'utilisateur. Enfin, le proxy, bien qu'il voit l'adresse IP de l'utilisateur, ne peut pas avoir d'information sur la requête DNS qui a été faites, étant donné qu'elle est chiffrée.

ODNS a été conçu pour être entièrement compatible avec l'infrastructure DNS existante, à quelques changements minimes près. Les expériences conçernant les performances d'ODNS révèle que la latence et la surcharge réseau avec ODNS sont minimes, et que les performances pour le trafic Internet des utilisateurs est acceptable.

Définitions :

Proxy : Un **serveur proxy** (appelé aussi **serveur mandataire** en français) est, dans le cadre des réseaux et d'internet, est une machine qui fait l'intermédiaire entre votre matériel (ordinateur, smartphone, tablette...) et internet. (https://www.astuces-aide-informatique.info/876/definition-proxy)