Hors dossier

Compte-rendu de la Journée 2017 du Conseil scientifique de l'AFNIC (Association française pour le Nommage Internet en Coopération)

Depuis sept ans, l'Association française pour le Nommage Internet en Coopération (AFNIC), gestionnaire historique du .fr, organise les Journées du Conseil scientifique de l'AFNIC (JCSA). Cet événement permet de faire un point sur les avancées en termes de recherche et standardisation sur les protocoles utilisés dans l'Internet, et plus particulièrement le *Domain Name System* ou DNS. Le DNS permet principalement de faire le lien entre les noms des équipements et les adresses utilisées par ceux-ci sur le réseau. Cette brique est fondamentale pour le fonctionnement de l'Internet, elle masque un objet technique comme une adresse IP (192.134.5.24) au profit d'un nom plus facilement exploitable par un être humain (afnic.fr). Au cours du temps, les fonctions du DNS ont été étendues, par exemple pour permettre de répartir la charge des sites web les plus fréquentés, de gérer des clés de chiffrement, d'enregistrer d'autres identifiants que les noms d'équipements... L'architecture du DNS est en constante évolution, pour à la fois augmenter les performances face à la croissance du nombre de requêtes, renforcer la sécurité de ce service critique et donc réduire l'impact des attaques, mieux protéger la vie privée, et ajouter des fonctionnalités en exploitant l'infrastructure robuste déjà déployée. Les membres du conseil scientifique étant proches des milieux universitaires et de la standardisation, ils contribuent à la réflexion de l'AFNIC sur les moyens à mettre au service de ses missions. Ils se prononcent sur les grandes orientations en matière de recherche et développement, de veille technologique et de gouvernance de l'Internet.

Après s'être intéressé les années précédentes à l'Internet des objets, aux architectures alternatives, à la métrologie et à la résilience, le conseil scientifique de l'AFNIC a traité le 6 juillet dernier de la gestion de la vie privée. Depuis la création du DNS dans les années 1980, les requêtes DNS successives menant à la résolution d'un nom n'ont jamais été chiffrées, et de plus elles remontent jusqu'à la racine. Des serveurs relais mis en place pour limiter le nombre d'interrogations masquent généralement l'identité de l'utilisateur, mais il peut arriver que l'information sorte d'un domaine ; pour une entreprise, cela peut conduire à une fuite d'informations confidentielles, comme par exemple la liste de ses fournisseurs. Ces problèmes peuvent être exacerbés, si les noms à résoudre contiennent des informations sensibles (par exemple, si ceux-ci incluent des identifiants obtenus en scannant des qr-codes, leur interception peut conduire à dévoiler un procédé de fabrication).

La JCSA a fait le point sur les différentes approches mises en œuvre par l'IETF (Internet Engineering Task Force), l'organisme international qui standardise les protocoles de l'Internet, pour diminuer les vulnérabilités du protocole liées à la gestion de la vie privée. Deux améliorations ont été proposées.

La première se base sur la nature hiérarchique des noms de domaines. Quand un utilisateur cherche à résoudre le nom « qrcode.ident.exemple.fr », la requête est envoyée à un résolveur qui est situé dans l'entreprise, chez son fournisseur d'accès ou chez un résolveur dédié (dit « ouvert ») comme en offrent Google, Cisco, etc. Celui-ci va interroger les serveurs « racines » du DNS pour

localiser les serveurs gérant la zone .fr, puis interroger ces serveurs pour localiser exemple.fr, et ainsi de suite, jusqu'à obtenir la réponse à la question.

Dans l'approche initiale, l'intégralité de la requête est fournie aux différents serveurs. Avec les extensions pour la gestion de la vie privée (dites « minimisation des requêtes »), seule la partie intéressant le serveur lui sera envoyée. Ainsi le serveur racine ne recevra qu'une requête concernant .fr, au lieu de qrcode.ident.exemple.fr

La deuxième amélioration concerne le chiffrement des requêtes entre la machine et le résolveur. Le changement majeur est le passage du protocole UDP (sans état) au protocole TCP (avec état) pour pouvoir utiliser le protocole de chiffrement TLS, utilisé également pour sécuriser les échanges du web. C'est de cette deuxième amélioration impliquant des changements protocolaires et comportementaux qu'a traité la JCSA.

La matinée de la JCSA est généralement dédiée à des tutoriaux. Sara Dickinson de Sinodun et Willem Toorop de NLnet Labs ont présenté et fait une démonstration du logiciel getDNS et de ses interfaces de programmation incluant les extensions pour la gestion de la vie privée. Maxence Tury de l'Agence nationale de la Sécurité des Systèmes d'Information (ANSSI) a présenté le fonctionnement du protocole TLS et, par le biais d'exemples interactifs avec le logiciel Scapy dans des machines virtuelles, a expliqué comment les certificats peuvent être utilisés pour chiffrer les communications.

L'après-midi a été consacré à des exposés des différentes technologies. Sarah Dickinson est revenue plus en détail sur les travaux de l'IETF dédiés à la gestion de la vie privée pour le DNS, et Alexander Mayrhofer, du registre nic.at, a présenté les premières études sur le dimensionnement des serveurs utilisant TLS. Il s'avère que les changements proposés auront peu d'impact sur les performances du DNS. Marck To, de la société EfficientIP, a ensuite réalisé une démonstration montrant comment des données peuvent être exfiltrées d'un site en utilisant le DNS, et quelles sont les méthodes pour se protéger de cette attaque. La dernière présentation du séminaire portait sur la thématique plus générale de la future application RGPD (Règlement général sur la Protection des Données de l'Union européenne), et son impact sur la conception des services a été abordé par Bruno Rasle de AFCDP.

L'ensemble des conférences de la journée (vidéos et supports de présentation) est accessible en ligne sur
https://www.afnic.fr/fr/l-afnic-en-bref/actualites/actualites-generales/10660/show/jcsa17-retour-sur-l-edition-2017-de-la-journee-du-conseil-scientifique-de-l-afnic.html