DNSSEC : sécurisation du DNS

Bureau du directeur de la technologie de l'ICANN

David Conrad
OCTO-006v3
24 juillet 2020

TABLE DES MATIERES

Ce document fait partie de la série de documents de l'OCTO. Veuillez consulter la page de publication de l'OCTO
pour obtenir la liste des documents compris dans la série. Si vous avez des questions ou des suggestions sur ces documents, veuillez les envoyer à octo@icann.org.

Cette révision contient des mises à jour de nombreuses personnes qui ont lu le document OCTO-006v2. L'ICANN apprécie beaucoup les commentaires qui nous ont été envoyés.

Introduction

Les extensions de sécurité du système des noms de domaine (DNSSEC) permettent de sécuriser le déplacement des informations sur Internet.

Le système des noms de domaine (*DNS*) est utilisé par tous les utilisateurs et par presque tous les dispositifs qui se connectent à l'Internet tous les jours. À l'aide d'un processus automatisé appelé *recherche* ou *résolution*, une des nombreuses fonctions du DNS est de traduire les noms faciles à mémoriser (par exemple, example.com) en numéros uniques appelés *adresses IP (Protocole Internet)* (par exemple 192.0.2.189 ou 2001:107A:61F7). Ces adresses IP sont ensuite utilisées par les périphériques pour s'identifier et communiquer entre eux. Ainsi, le DNS est souvent comparé à un répertoire téléphonique ou à une liste de contacts, où les noms sont traduits en numéros.

Qu'est-ce que les DNSSEC ?

Lorsque le DNS a été créé au début des années 1980, la sécurité n'était pas un aspect primordial de la conception. À cause d'une décision de conception qui avait du sens à l'époque, dans de rares cas, les attaquants pouvaient fournir leurs propres réponses aux recherches de noms de domaine au lieu de ce que le propriétaire du domaine (le titulaire) avait demandé. Par exemple, au lieu d'accéder au site Web que vous avez demandé dans votre navigateur, un attaquant pourrait compromettre les messages du DNS pour vous rediriger vers un site Web qui ressemble au site Web auquel vous avez voulu accéder, mais qui est contrôlé par l'attaquant. Dans les années 1990, la communauté technique du DNS a trouvé la solution définitive à ce problème, connue sous le nom d'extensions de sécurité du système des noms de domaine ou *DNSSEC*.

Comment fonctionnent les DNSSEC ?

Un titulaire de nom de domaine est la personne ou l'organisation qui contrôle l'information associée à un nom de domaine, c'est-à-dire la correspondance nom-adresse et d'autres données. Les DNSSEC permettent aux titulaires de noms de domaine de signer numériquement les informations qu'ils ont introduites dans le DNS ; cela permet aux clients (par exemple, votre navigateur Web) de vérifier que les réponses du DNS qu'ils reçoivent en réponse aux demandes de recherche n'avaient pas été modifiées depuis leur signature.

En 2010, l'ICANN a permis au niveau le plus élevé du DNS, connu sous le nom de racine, d'être signé par les DNSSEC, facilitant ainsi considérablement le déploiement des DNSSEC à l'échelle mondiale. Cependant, même une décennie plus tard, le déploiement des DNSSEC continue de prendre du retard.

Quels sont les avantages du déploiement des DNSSEC ?

- **Les DNSSEC protègent l'Internet** : étant donné que le DNS est essentiel au fonctionnement de l'Internet, la protection des données fournies par le DNS est critique. Par analogie, le DNS peut être considéré comme des « panneaux routiers » sur Internet, car il permet de diriger la communication vers le contenu ou le service approprié. Comme dans le cas des panneaux routiers sur les routes réelles, si les attaquants changent la destination qui y est indiquée, cela pourrait entraîner un trafic mal acheminé, vous redirigeant vers un quartier dangereux de la ville.

- **Les DNSSEC protègent les utilisateurs finaux** : les DNSSEC peuvent assurer que les données du nom de domaine reçues par les utilisateurs finaux soient identiques à celles que le titulaire du nom a voulu envoyer à l'utilisateur final. Les DNSSEC aident à s'assurer que lorsqu'un utilisateur final ou un dispositif tente d'accéder au contenu ou au service pointé par un nom de domaine, le site avec lequel il communique soit celui prévu par le titulaire du nom de domaine.

- **Les DNSSEC protègent les entreprises, les organisations et les gouvernements** : les DNSSEC réduisent la probabilité que les utilisateurs finaux qui souhaitent utiliser leurs services ou afficher leur contenu soient mal dirigés vers un site où ils pourraient éventuellement être escroqués par un attaquant. Les fournisseurs de services Internet (FSI) peuvent ajouter de la valeur au service qu'ils fournissent à leurs clients en activant la validation des DNSSEC sur leurs résolveurs. Les organisations qui signent leurs noms de domaine avec les DNSSEC réduisent le risque que les personnes qui les recherchent sur Internet soient mal redirigées.

- **Les DNSSEC favorisent l'innovation** : les DNSSEC sont un outil pour vérifier et protéger les données du DNS, ce qui permet de faire confiance à ces données. Cela permet à tour de rôle de tirer parti du DNS global pour créer une base de données de nom/valeur sécurisée (par exemple, vous soumettez un nom et le DNS renvoie des valeurs associées à ce nom) qui est distribuée à l'échelle mondiale et accessible publiquement, c'est à dire par n'importe qui sur Internet. Par conséquent, cette base de données sécurisée peut créer des possibilités d'innovation et permettre de nouvelles technologies, services et installations. Par exemple, la technologie d'authentification d'entités nommées basée sur le DNS (DANE), crée une nouvelle façon de sécuriser les connexions sur Internet. DANE tire profit des données protégées par les DNSSEC dans le DNS et corrige certaines des vulnérabilités de la façon actuelle d'établir des connexions sécurisées sur Internet. Cela rend le commerce et les communications sur Internet plus sécurisés.

Comment mettre les DNSSEC en action ?

De manière générale, le DNS a deux aspects : d'une part, la publication, qui est effectuée par les titulaires des noms de domaine ou leurs agents et, d'autre part, la recherche (également appelée résolution) qui est généralement effectuée par des opérateurs de réseau tels que les fournisseurs de services Internet. Pour bénéficier des DNSSEC, les deux acteurs impliqués doivent l'utiliser.

- **Titulaires de noms de domaine :** les personnes responsables de la publication des informations du DNS doivent s'assurer que leurs données du DNS soient signées par les DNSSEC. Historiquement, ce processus a en général été assez compliqué et

susceptible d'erreurs. Cependant, de nos jours, la plupart des paquets de logiciels DNS modernes et des systèmes d'enregistrement possèdent des outils qui automatisent la signature DNSSEC des données que les titulaires de noms de domaine souhaitent publier. Par conséquent, les titulaires de noms de domaine ou leurs agents doivent simplement activer la signature DNSSEC dans leurs serveurs DNS (ou dans leurs bureaux d'enregistrement) et fournir à leur bureau d'enregistrement un peu d'information, connue sous le nom *de registre relatif au signataire de la délégation*, pour aider à établir la confiance dans l'information qu'ils viennent de signer.

- **Opérateurs de réseau :** du côté de la recherche, cela est encore plus facile : les opérateurs de réseau doivent uniquement activer la validation des DNSSEC sur les résolveurs qui gèrent les recherches DNS pour les utilisateurs. Le logiciel des résolveurs permet de plus en plus la validation des DNSSEC par défaut.

- **Utilisateurs finaux de l'Internet :** en général, les utilisateurs finaux n'ont pas besoin de faire autre chose qu'encourager leurs opérateurs de réseau à permettre la validation et la signature des DNSSEC des domaines qu'ils utilisent.

Quels sont les coûts associés aux DNSSEC ?

Les serveurs DNS doivent prendre en charge les DNSSEC, tant du côté de la publication que de celui de la recherche. Il peut donc être nécessaire que les entreprises mettent à jour leurs paquets de logiciels DNS (une meilleure pratique que les DNSSEC soient déployés ou pas).

- Du côté de la publication, il peut également être nécessaire que les titulaires de nom de domaine ou leurs agents modifient leurs processus pour permettre que les registres relatifs au « signataire de la délégation » soient envoyés à leur bureau d'enregistrement. Le coût de ces modifications peut être considérable ; mais celles-ci ne se produiraient qu'une seule fois et le coût serait donc unique.

- Du côté de la recherche, en supposant que le logiciel du serveur DNS soit raisonnablement moderne, les coûts devraient être négligeables, car il ne faudrait qu'une modification de configuration pour permettre la validation des DNSSEC.

Que se passe-t-il si je ne déploie pas les DNSSEC ?

- **Les utilisateurs pourraient être vulnérables aux attaques :** si une organisation choisissait de ne pas déployer ou activer les DNSSEC, ses utilisateurs seraient susceptibles de recevoir un type d'attaque en particulier, dénommé « empoisonnement du cache ». Lorsqu'un utilisateur final effectue une recherche, les attaquants pourraient insérer de manière transparente des réponses aux questions sur le DNS, ce qui pourrait rediriger les tentatives de communication vers des dispositifs contrôlés par les attaquants. Les attaquants pourraient alors imiter des sites Web ou d'autres services, dérober des noms d'utilisateur et des mots de passe, etc. Les réponses incorrectes

seraient également conservées sur le serveur effectuant la recherche pendant un certain temps, ce qui entraînerait la redirection jusqu'à ce que les réponses expirent ou soient supprimées. Alors que ces types d'attaques sont rares, étant donné que les DNSSEC existent pour y répondre et sont disponibles depuis un certain temps, les organisations qui deviennent des victimes de cette exploitation peuvent avoir des discussions difficiles avec leurs utilisateurs sur la raison pour laquelle ils n'ont pas déployé les DNSSEC. Étant donné que d'autres formes d'attaques sont empêchées, il est probable que les attaquants profitent des sites qui n'ont pas déployé les DNSSEC, car la mise en œuvre d'attaques via le DNS devient plus courante.

- **L'innovation pourrait être ralentie :** le non-déploiement des DNSSEC entrave l'innovation et ralentit le déploiement de nouvelles technologies qui utilisent le DNS comme base de données de confiance à l'échelle mondiale. Certaines de ces technologies promettent de fournir de meilleures façons de faire confiance aux connexions pour les services Internet, tels que le courrier électronique ou le Web.

Bien que les vulnérabilités traitées par les DNSSEC aient existé depuis la création du DNS, il n'y a pas encore eu de nombreuses attaques de haut profil qui tirent parti de ces vulnérabilités. Pour cette raison, certains peuvent croire que les coûts de déploiement des DNSSEC l'emportent sur les avantages qu'elles offrent. Il convient toutefois de noter que les coûts et les risques liés à la mise en œuvre des DNSSEC ont considérablement diminué. En fait, les avantages des DNSSEC augmentent au fur et à mesure de leur déploiement dans un plus grand nombre de réseaux.

Une autre façon d'examiner la question du déploiement des DNSSEC : « S'il vaut la peine de mettre des données dans le DNS, ne vaut-il pas la peine de s'assurer que les données ne soient pas faussées ? »

Quelques antécédents des DNSSEC

En 1983, Paul Mockapetris de l'Institut des sciences de l'information de l'Université de Californie du Sud a publié une série de documents qui ont introduit le concept du système de noms de domaine. Dans sa forme originale dans les années 1980, le DNS n'avait pas de sécurité, de confidentialité ou d'authentification intégrées ; il n'y avait pas de mécanisme pour s'assurer qu'une réponse reçue était légitime et correspondait effectivement à la question posée.

Vers 1990, Steve Bellovin, d'AT&T Bell Laboratories, a rédigé un article qui décrivait comment les attaquants pourraient tirer parti d'une décision de conception particulière dans le DNS pour pénétrer dans les systèmes. Dans son article, Bellovin a recommandé l'utilisation de l'authentification cryptographique pour mieux protéger le DNS. À la suite de la publication de l'article de Bellovin, un processus formel a commencé à faire de sa proposition une norme du protocole de l'IETF (Groupe de travail de génie Internet) dénommée « Améliorations à la sécurité du DNS » (*DNSSEC)*.

Le logiciel DNS qui a mis en œuvre les DNSSEC a été initialement développé à la fin des années 1990, avec quelques premiers déploiements des DNSSEC à partir de l'an 2000, y compris par le populaire ccTLD .SE (le code de pays de la Suède). Toutefois, ces déploiements précoces ont révélé de nombreux défis techniques pour l'opération des DNSSEC à grande

échelle dans la production, ce qui a conduit l'IETF à continuer à travailler à l'amélioration du protocole au cours des huit années suivantes.

Rien de majeur ne s'est produit en termes de déploiement jusqu'en 2008, quand un chercheur en sécurité appelé Dan Kaminsky a découvert une sérieuse lacune de conception dans le protocole DNS lui-même qui a permis aux attaquants de lancer des attaques par empoisonnement du cache contre le côté de la recherche du DNS. Cette constatation a suscité de nouvelles tentatives de la communauté technique du DNS pour obtenir davantage de déploiement des DNSSEC, et en particulier, pour obtenir la racine du DNS signé.

En juillet 2010, la zone racine a été signée pour la première fois par l'ICANN, fournissant un point d'ancre de confiance global pour toute validation des DNSSEC. En octobre 2018, la clé de signature de clé de la zone racine a été mise à jour avec succès pour la première fois, ce qui représente un jalon important pour les DNSSEC.

Une série de campagnes internationales de détournement du DNS en 2018 et 2019 a conduit à la toute première directive de l'Agence de cybersécurité et de sécurité des infrastructures des États-Unis (US-CERT), et a conduit l'ICANN à renouveler son appel pour que toutes les parties prenantes du DNS déploient entièrement les DNSSEC.

Le rôle de l'ICANN dans les DNSSEC

L'ICANN, dans le cadre de sa mission visant à promouvoir un écosystème DNS plus stable, plus sûr et plus résilient, est depuis longtemps un des principaux promoteurs du déploiement des DNSSEC. Les contrats de fonctionnement officiels de l'ICANN avec les opérateurs de registre et les bureaux d'enregistrement exigent que les DNSSEC soient pris en charge. L'organisation ICANN s'engage régulièrement avec les parties prenantes du DNS du monde entier pour les aider à comprendre l'importance des DNSSEC et pour former les ingénieurs dans le déploiement et l'opération des DNSSEC dans leurs réseaux. En plus de la sensibilisation et du renforcement des capacités, les technologues de l'ICANN travaillent avec la communauté de l'IETF sur les améliorations des DNSSEC.

Du point de vue opérationnel, l'ICANN continue de jouer un rôle essentiel. L'ICANN est responsable de la génération, du stockage et de la mise à jour périodique de la clé de signature de clé de la racine, une clé cryptographique approuvée par tous les résolveurs validants sur Internet, qui est utilisée dans le processus pour signer la racine du DNS global.

Pour en savoir plus

Il existe de nombreuses ressources et groupes techniques impliqués dans les DNSSEC et leur déploiement. Quelques exemples :

- Les DNSSEC et tous les autres efforts liés au protocole DNS sont discutés au sein de l'IETF, en particulier dans le Groupe de travail sur les opérations du DNS (DNSOP).
- Les ateliers DNSSEC ont lieu trois fois par an, lors des réunions publiques de l'ICANN. Ces ateliers, organisés par l'Internet Society, fournissent des informations opérationnelles, des conseils et des analyses sur le déploiement des DNSSEC. Un site

Web associé parrainé par l'Internet Society fournit une archive de ces réunions.

- Pour plus d'informations, l'ICANN fournit une description générale des DNSSEC et explique pourquoi il s'agit d'une question importante.