MONTREAL – DNSSEC pour tous : un guide pour débutants
Dimanche 3 novembre 2019 – 17h00 à 18h30 EDT
ICANN66 | Montréal, Canada

DAN YORK : ... qui sont là pour vous faire cette présentation.

Nous allons avoir des questions et réponses qui vont être posées plus tard. Alors approchez-vous, la salle est immense, venez, n'hésitez pas. Nous avons des micros.

Je m'appelle Dan York. Je suis avec l'Internet Society et je suis impliqué dans le travail qu'effectue l'Internet Society. Ce dont on va vous parler maintenant, c'est ce que l'on veut dire lorsqu'on parle du DNSSEC, quel est l'objectif du DNSSEC. Nous allons vous raconter une petite histoire, nous allons vous faire des sketchs et nous allons en fait s'amuser en ce dimanche soir.

Premièrement, quelques questions. Combien d'entre vous ont déployé le DNSSEC d'une manière ou d'une autre ? Quelques personnes. Combien de personnes ne savent absolument pas de quoi il s'agit ? Il y en a quelques uns. Je vois qu'il y a même des chevauchements entre ces différentes réponses. Donc on va revenir aux origines du DNSSEC, en 5000 av. JC.

Donc voilà l'histoire. Vous avez Ugwina qui habite dans une grotte d'un côté du Grand Canyon et voilà Og, il habite dans une grotte qui est de l'autre côté du Grand Canyon. Le problème, c'est que la

distance est longue donc en fait, ils ne se parlent pas beaucoup, ils ne se rendent pas beaucoup visite. Mais lors d'une de leurs visites, ils se rendent compte qu'il y a de la fumée qui se dégage du feu de Og. Donc en fait, ils se rendent comptent qu'ils peuvent communiquer en utilisant des signaux de fumée. Ils s'envoient des signaux de fumée de manière à pouvoir se raconter des histoires, vraiment avoir une conversation.

Mais un jour, il y a un autre homme de Cro-Magnon qui s'appelle Kaminski, qui emménage à côté de chez de Og et qui commence à envoyer ses propres signaux de fumée. Soudain, Ugwina de l'autre côté n'arrive pas à comprendre avec qui elle doit communiquer, quels sont les bons signaux. Donc elle se dit : « Je pars en voyage. Je vais essayer de voir ce que je peux faire, comment est-ce que je peux identifier quel est le bon signal de fumée. »

Donc ils vont consulter les sages et l'homme des cavernes Diffie se dit : « J'ai une idée. » Il se précipite dans la grotte de Og et va tout au fond et voit une pile de sable bleu. C'est assez étrange, cela n'existe que dans la grotte de Og. Donc il prend son sable, il le jette sur le feu et le feu devient bleu, une couleur magnifique. Et tout d'un coup, ils peuvent communiquer, Ugwina sait quels sont les signaux qui viennent de Og. Personne ne peut plus interférer dans la conversation parce que tout le monde sait que c'est la fumée bleue qui vient de Og.

Ce qui est quand même marrant, c'est que c'est de cela dont il s'agit dans la DNSSEC. Il s'agit de s'assurer qu'on reçoit bien les bonnes

informations de l'expéditeur. L'idée, c'est de faire quelque chose avec les informations pour voir ce qui vient de cette personne.

Alors on va passer à la partie un peu plus technique, à haut niveau. Voilà un petit peu à quoi ressemble le DNSSEC. On a la racine du DNS, on a tous ces domaines de premier niveau, ces TLD qui sont là sous différentes formes. Et on a les domaines de deuxième niveau en-dessous, et on a tout ceci qui se passe.

Le résolveur de DNS sait comment atteindre la zone racine et il sait comment passer par la hiérarchie. Et à chaque niveau, le résolveur lui dit d'aller parler à quelqu'un d'autre. Entre fait, le DNS est une base de données distribuée. Il y a un système de cache et un système de flux d'information pendant tout le cheminement. Mais le problème, c'est qu'il n'y a pas de sécurité dans le protocole. Comme dans la petite histoire, il y a quelqu'un d'autre qui peut venir et usurper et donner d'autres réponses, d'autres manières. Vous pouvez empoisonner les caches du résolveur parce qu'une fois que les informations sont stockées, on peut les conserver pendant un certain temps.

Donc nous allons maintenant vous faire un petit sketch. Vous allez voir, venez sur la scène, nous allons vous montrer un petit peu à quoi cela ressemble. Donc ce que vous allez voir, c'est nos personnages qui vont jouer le rôle de l'internaute qui va chercher des informations, qui veut se connecter à bigbank.com. Voilà, notre petite troupe d'acteurs est en train de se mettre en place, parfait.

Wes Hardaker sera notre internaute qui va parler à notre FSI, un résolveur, et ce résolveur va ensuite entrer en lien avec notre hiérarchie du DNS qui est là.

On a besoin du micro s'il vous plaît. Ça y est, c'est bon.

WES HARDAKER : J'aimerais m'acheter un yacht. J'ai toujours eu envi de m'acheter un yacht. C'est vraiment des bateaux magnifiques, donc je pense qu'il faut que j'aille voir ma banque. Ma banque s'appelle www.bigbank.com et je vais aller voir combien d'argent j'ai dans ma banque. Est-ce que vous pouvez me donner l'adresse pour www.bigbank.com pour que je puisse aller parler à ma banque ?

WARREN KUMARI : Oui, vous êtes justement le type de client que j'aime garder heureux, donc je vais aller voir ce qui se passe.

Bonjour racine, j'ai un internaute qui veut se rendre sur www.bigbank.com. Est-ce que vous pouvez me dire où est-ce que cela se trouve ?

FRED BAKER : J'aimerais bien pouvoir mais j'ai un problème : je ne sais pas. En fait, je sais où trouver le .com. Vous pouvez donc demander au .com.

WARREN KUMARI : D'accord, merci, je vais essayer.

Bonjour .com. Un de mes internautes veut se rendre sur www.bigbank.com. Est-ce que vous pouvez me dire où c'est ?

ORATEUR NON-IDENTIFIÉ : Je ne sais pas où se trouve le www mais par contre, le bigbank.com est là.

WARREN KUMARI : Bonjour bigbank. Est-ce que vous pouvez me dire où se trouve le www.bigbank.com ?

RUSS MUNDY : Bonjour monsieur FSI. Je peux vous dire où le www.bigbank.com se trouve : c'est au 2.2.2.3.

WARREN KUMARI : Super, j'ai la réponse.

Bonjour monsieur l'internaute, voilà où se trouve le www.bigbank.com : c'est au 2.2.2.3. D'ailleurs, est-ce que je pourrais monter dans votre yacht ?

WES HARDAKER : Désolé, dans mon yacht, il n'y a pas de résolveurs récursif. Super, j'ai énormément d'argent, assez pour m'acheter un bateau.

DAN YORK : On les applaudit. Donc voilà comment fonctionne le DNS, voilà ce qui se passe constamment pour toutes les petites requêtes de DNS qui sont effectuées.

Maintenant, nous allons voir un petit peu comment cela pourrait se passer. Nous allons donc demander aux personnages de refaire le sketch.

WES HARDAKER : C'est parti, je vais m'acheter mon super yacht. Je vais donc aller à bigbank.com de manière à transférer mon argent. Je ne sais plus où c'est. Vous pouvez me dire où c'est ?

WARREN KUMARI : Oui, moi aussi j'ai oublié mais je vais me débrouiller pour trouver l'information.

Bonjour racine. Un de mes internautes veut aller au www.bigbank.com. Vous pouvez me dire où c'est ?

FRED BAKER : Si seulement je connaissais la réponse. Je sais où se trouve le .com par exemple. Est-ce que cela vous aide ?

WARREN KUMARI : Oui, on va aller voir.

Bonjour .com. Un de mes internautes veut aller au www.bigbank.com. Vous pouvez me dire où c'est ?

ORATEUR NON-IDENTIFIÉ : Je ne sais pas. Mais je sais que bigbank.com se trouve au 2.2.2.2.

WARREN KUMARI : Je vais demander.

ANDREW MCCONACHIE : Je sais. Le bigbank.com, c'est au 6.6.6.6

WARREN KUMARI : Super. Voilà monsieur l'internaute.

WES HARDAKER : 6.6.6.6, génial, je vais pouvoir donner tout mon argent au 6.6.6.6. Merci. Et mon bateau, il est où ?

ANDREW MCCONACHIE : Merci.

WES HARDAKER : Mon bateau ?

DAN YORK : On les applaudit.

Donc pour le DNS, dont on parle dans cette présentation, voilà comment on peut l'empoisonner et avoir des attaques. Donc le résolveur peut recevoir ces deux premières réponses et à ce moment-là, c'est une question de rapidité, qui peut donner la réponse. Donc en fait, le mauvais, le diable est arrivé avant que la réponse ne soit donnée.

En partie, le danger, c'est également que Warren, qui a le chapeau, notre FSI, va conserver cette réponse pendant un certain temps. Donc toutes les autres personnes qui posent la question du www.bigbank.com, ces personnes vont continuer de recevoir cette mauvaise réponse ; ils vont tous la recevoir jusqu'à ce que cela se termine. Donc c'est cela les attaques du DNS, c'est cela les empoisonnements du cache. Voilà exactement ce qui se passe.

Ce que nous avons maintenant encore une fois, c'est le DNS. Avec le DNSSEC, on ajoute le concept de la signature numérique. On va demander à la troupe de rester là parce qu'ils vont à nouveau nous faire ce sketch. Mais ce qui se passe, c'est que vous avez des clés, des signatures qui sont stockées à l'intérieur du DNS de manière à pouvoir vérifier que les informations viennent bien de la source, est-ce qu'il s'agit vraiment de la bonne source d'information pour le www.bigbank.com. Donc le résolveur, pour que cela fonctionne, sait où se trouve la clé de la racine. Je ne sais pas si vous avez entendu parler de roulement de clé l'année dernière ? Oui ? L'idée, c'était de s'assurer qu'il y a une chaîne de confiance de la racine du DNS sur toute la chaîne. Donc tout est lié de manière à protéger l'intégrité des informations. L'idée, c'est que notre serveur de nom bigbank est bien

celui qui donne les informations au FSI, que ce n'est pas quelqu'un d'autre qui les donne.

Donc on va redemander à notre troupe de revenir ici et on va refaire le sketch, cette fois-ci avec le DNSSEC.

WES HARDAKER : Alors, vous allez être contents parce que c'est le dernier sketch.

DAN YORK : Alors, qu'est-ce qu'on fait avant de commencer ? Il faut signer la racine. Si seulement c'était aussi facile que cela. Vous voyez que maintenant, les racines ont signé ; le bigbank a signé, le .com a signé, tout le monde a signé.

WES HARDAKER : J'ai encore besoin d'un autre yacht. Le bigbank.com, c'est où cette fois-ci ? Et est-ce que vous pourriez s'il vous plaît faire attention à ne pas faire d'erreur.

WARREN KUMARI : Bon, je vais faire de mon mieux. Je vais demander à la racine.

Bonjour racine. Un de mes internautes voulait savoir où se trouve le www.bigbank.com. Est-ce que vous pouvez me le dire ?

FRED BAKER : Non, je ne peux pas mais je peux vous dire où se trouve le .com et le .com pourra peut-être vous le dire. Et en plus, je suis signé.

WARREN KUMARI : Attendez, je vérifie la signature... Pas mal, ça a l'air valide. Je vais voir avec le .com

Bonjour .com. Un de mes internautes veut acheter un bateau. Il veut savoir où se trouve bigbank.com. Est-ce que vous pouvez me dire où cela se trouve ?

ORATEUR NON-IDENTIFIÉ : Je ne sais toujours pas où se trouve le www., mais le bigbank.com se trouve au 2.2.2.2 et je peux signer ma réponse.

WARREN KUMARI : Je vérifie la signature. C'est bon. Je vais donc lui poser la question.

Bonjour www.bigban.com.

ANDREW MCCONACHIE : Bonjour.

WARREN KUMARI : Comment ça va ?

ANDREW MCCONACHIE : C'est au 6.6.6.6.

WARREN KUMARI : Où est la signature ? Je ne vois pas de signature. Bigbank.com, vous pouvez me dire où se trouve le www.bigbank.com ?

RUSS MUNDY : Oui, tout à fait. Cela se trouve au 2.2.2.3 et en plus, je signe.

WARREN KUMARI : Je vérifie mais je vais vraiment faire attention cette fois-ci. Oui, c'est bon. C'est bon monsieur l'internaute, voilà le www.bigbank.com, il se trouve au 2.2.2.3. Et j'ai validé, vous pouvez me faire confiance.

WES HARDAKER : Super. Madame la banque, est-ce que vous pouvez transférer tout mon argent ? Je veux acheter un bateau à Dan.

DAN YORK : Merci Wes, c'est très sympa. Allez, on les applaudit.

Donc voilà comment cela fonctionne. Voilà ce qu'est le DNSSEC. L'idée, c'est d'avoir ces signatures qui garantissent que personne d'autre ne peut s'immiscer dans le processus. Voilà ce que fait le DNSSEC et c'est tout ce qu'il fait, mais c'est très important. Le DNSSEC garantit l'intégrité des informations.

Ce que le client reçoit, c'est ce qui a été mis dans le DNS. Ce n'est pas une question de confidentialité, c'est uniquement de vérifier que les informations correspondent à ce que l'internaute a mis dans le DNS.

Nous allons maintenant vous donner quelques exemples avec Russ Mundy qui va venir faire la présentation. Je vais rendre à Wes son argent.

RUSS MUNDY : Merci Dan et merci à vous tous qui êtes avec nous cet après-midi. Vraiment, c'est très lumineux ces projecteurs. Alors super, je vais pouvoir faire avancer les diapositives. Je vais vous donner des exemples et des descriptions de ce à quoi il faut penser lorsque l'on passe par le processus de déploiement du DNSSEC.

La raison pour laquelle il faut le faire et la raison pour laquelle on s'en inquiète du DNS, c'est du point de vue de informations ; surtout lorsque le DNSSEC n'est pas en place en fait, il peut y avoir perturbation des informations.

Mais pourquoi est-ce que les gens attaquent le DNS ? Parce que le DNS n'est pas aussi intéressant que cela. Mais les gens attaquent le DNS dans la plupart des cas pour pouvoir en fait agir sur les applications sans vraiment effectuer des requêtes de DNS. Comme vous l'avez vu tout à l'heure, Wes voulait transférer de l'argent. Vous avez vu qu'il y avait une tentative de vol de l'argent. L'idée, c'est vraiment d'attaquer des applications qui utilisent le DNS. Donc si vous n'arrivez pas au bon endroit, qui sait ce qui va se passer.

Donc, nous avons vu de multiples exemples dans la réalité de ce type de situation ; certaines sont affichées à l'écran. Toutes les applications qui fonctionnent sur l'internet actuellement sont très susceptibles d'utiliser le DNS. Donc la plupart du temps, les utilisateurs de l'application ne savent pas et finalement, peu leur importe de savoir si le DNS est présent ou pas. Mais pourtant, le DNS est essentiel pour que leur application fonctionne correctement.

Il y a quelques années, je suis revenu sur ces informations mais je n'ai pas gardé le détail de ce que j'avais trouvé. Mais il y a quelques années, il y avait un professeur d'université qui faisait un cours sur la programmation et il demandait à ses étudiants d'écrire un programme de piratage du DNS. J'ai regardé tous les prérequis pour le cours et je n'ai rien vu dans toutes cette description sur la déontologie ou sur le fait que peut-être qu'il ne faudrait pas faire ce type de choses. C'était simplement : « Chers étudiants, rédigez un programme de piratage du DNS. » Cela fait peur. Heureusement, au cours des cinq années passées, je n'ai pas trouvé le même type d'information. Donc apparemment, cela s'est calmé.

Comme Dan l'a dit, ce qui est important, c'est de pouvoir arriver au bon endroit et lorsqu'on arrive au bon endroit, de pouvoir vérifier que les informations que l'on reçoit sont bien justes. Donc la clé cryptographique publique qui est intégrée pour que le DNSSEC fonctionne, c'est le mécanisme technique qui sous-tend tout ceci.

Lorsqu'on a effectué les efforts préliminaires aux réunions de l'ICANN, on a effectué de vrais piratages. Donc voilà quelques diapositives qui

vous présentent un petit peu la même idée que ce que vous avez pu voir dans le petit sketch sur la scène.

Une des raisons pour lesquelles on a arrêté de le faire en vrai en fait, c'est que lors d'une des réunions, on a réussi ; plutôt que de pirater le DNS dans la salle spécifique, étant donné la configuration du réseau qui n'était pas exactement ce à quoi on s'attendait, on a piraté le DNS pour toute la réunion de l'ICANN. C'était assez drôle à ce moment-là, après, une fois fait mais au moment même, ce n'était pas très drôle.

Joe, l'utilisateur que vous voyez en bas de l'écran à gauche, veut aller sur son serveur web. Et comme vous le voyez sur l'écran, vous voyez qu'il envoie une requête, une demande qui va vers son serveur récursif qui lui-même l'envoie au serveur qui fait autorité. Il envoie sa réponse au serveur récursif et ensuite, le serveur récursif renvoie l'information à l'utilisateur. Voilà, c'est ce que vous avez vu tout à l'heure à travers le sketch que l'on a mis sur scène. Une fois que cela est fait, il peut continuer avec sa transaction.

Nous mettons cela sur un site web. Vous voyez à l'écran la configuration que l'on utilise, ce que vous pouvez voir sur l'écran en lui-même. Il n'y a pas de formule standardisée mais c'était l'idée, de mettre une indication qui prouvait que cela avait été vérifié avec le DNSSEC. Lorsque l'on n'utilise pas la validation DNSSEC ou son mécanisme, vous allez avoir un symbole totalement différent comme vous voyez sur l'écran, avec la petite marque verte en haut à gauche et ensuite, vous avez la page avec le triangle jaune qui dit que le DNSSEC

n'est pas en place. C'est ce qu'on vous a montré tout à l'heure sur la scène.

Comme vous voyez, Joe l'utilisateur envoie une demande mais cette fois-ci, le diable est sur le réseau. Donc la demande part comme cela et dans le vrai monde, vous savez, le diable voit cette demande et fournit une réponse malgré que cette demande continue tout de même à se déplacer à travers le réseau. Mais Joe l'utilisateur est envoyé vers le mauvais site web. Vous voyez les autres requêtes sont revenues avec une réponse mais Joe l'utilisateur n'a pas reçu cette réponse car le résolveur qu'il a utilisé lui a envoyé une fausse réponse. Donc cette requête est allée au mauvais site web.

Il ne peut pas passer à travers tout cela à moins d'utiliser le DNSSEC. Le DNSSEC empêcherait de recevoir cette mauvaise réponse ; il obtiendrait la bonne réponse et par la suite, il pourrait revenir vers le bon site web et obtenir les informations comme prévu.

Nous avons donc mis en place un site web pour montrer ce qui peut être fait. D'ailleurs ce site web avait été construit de façon à montrer qu'il y avait une section de ce site web qui montrait en emplacement où il pouvait y avoir un piratage. Nous avons utilisé un moteur de recherche qui n'utilisait pas le DNSSEC. Nous avons inséré là des informations et ces informations étaient de fausses informations et cela disait : « Steve Crocker a admis que le DNSSEC ne résoudrait pas la faim dans le monde. » Vous voyez ? Donc c'était une illustration humoristique.

Mais comme vous le voyez sur l'écran, le DNSSEC n'était pas présent. Et là-haut sur l'écran à gauche, vous voyez un autre titre qui dit : « .org a partagé les avis DNSSEC avec Comcast. » Là, ce site était vérifié. Donc avec le piratage, nous avons rajouté des informations sur une page. Même si c'était la même page sur le moteur de recherche, l'information qui s'y trouvait était complètement différente donc il y avait de fausses informations qui avaient été intégrées sur une page web. Donc quand on passe d'un serveur de noms de domaine qui soit vide, sans information de cache par exemple comme vous voyez à l'écran... Cnn.com, il y a quelques années, il y avait 75 à 100 demandes juste pour construire une page. Et toutes ces demandes peuvent être piratées, bien sûr.

Est-ce que c'est mieux maintenant ? Pas forcément. D'une certaine manière oui mais d'une autre, non. Pour construire une page d'un site comme celui-ci, comme vous le voyez à l'écran, cette instrumentation démontre qu'il y a des signatures DNSSEC mais cela prend beaucoup de travail, cela prend énormément de temps. Les inquiétudes des gens sont souvent basées sur des choses comme les clés cryptographiques et tout cela. Il y a beaucoup de choses qui sont importants mais malgré tout, ce sont les données de zone du DNSSEC qui sont importantes.

Il faut absolument s'assurer que toutes les informations soient adéquates. Il faut que le DNSSEC soit associé à toutes les zones pour que les utilisateurs qui obtiennent des informations sachent que l'information qu'ils obtiennent est correcte. Donc si vous faites très attention à votre clé cryptographique, les personnes qui essaierons

d'attaquer votre système attaqueront les parties de votre système qui envoient les informations. Si vous signez ces informations, la personne qui va recevoir les informations saura que les informations sont correctes. Mais dans le cas des attaques qui ont réussi, les gens ont reçu les mauvaises informations. Donc en fait, si vous ne faites pas les choses comme il le faut, vous en tant qu'opérateurs, vous devez vraiment vérifier que cette information est correcte. Sinon, la faute sera la vôtre parce que vous n'avez pas géré les informations de façon adéquate.

Voilà un autre exemple du DNS sans le DNSSEC. Vous saisissez les informations dans votre serveur qui fait autorité. Cette information rentre. Le serveur qui fait autorité contient ces informations et reçoit donc une requête du serveur récursif et il répond à cette demande.

Si vous incluez le DNS dans vos opérations, et contrairement à l'outsourcer ou avoir un opérateur qui le fait pour vous, vous allez le faire vous même et vous n'allez pas demander qu'un opérateur de registre se préoccupe de cela. Vous allez pouvoir faire vos propres opérations. Vous devez avoir certainement des personnes expertes sur le DNS. Et pour faire ces activités DNSSEC, il faut que vous ayez quand même des personnes qui sont expertes sur le sujet. Si vous avez votre propre DNS, il serait bon de faire le DNSSEC en interne.

Si vous êtes un grand TLD ou si vous êtes un opérateur de registre ou une grosse entreprise comme on le voit ici avec l'exemple de hp.com, verisign.com, ce sont des entreprises qui sont liées au DNS. Ce sont

des organisations qui sont importantes et qui vont faire leur propre DNSSEC.

Si vos zones DNS qui ne sont pas si importantes vis-à-vis de l'internet ou du moins dans votre organisation, ici je prends un exemple, net-snmp.org. Ils n'ont pas d'activités qui sont liées au DNS. Donc ils n'ont pas des opérations qui sont critiques au niveau du DNS, elles ne sont pas critiques à l'internet ou aux fonctions de votre affaire. Dans ce cas-là, quand on dit qu'on utilise le DNS, il faut utiliser le DNSSEC quand c'est possible. La chose la plus importante, c'est de protéger les données de la zone DNS.

Maintenant, on a vu un exemple pour tout ce qui était de la zone qui fait autorité. Là, on va parler des requêtes pour les informations.

Comme vous voyez, il y a une illustration à l'écran qui montre les étapes qui doivent être entreprises à certains endroits. Il faut signer donc les données pour la zone avant que ces données soient chargées sur le serveur qui fait autorité. Ensuite, le serveur récursif lui-même a besoin d'avoir la clé de la racine et de faire la validation parce qu'ainsi, une fois que les requêtes sont faites et que les réponses reviennent, la validation peut être effectuée. Cela peut être fait avec une configuration ; c'est assez simple.

En résumé, on peut dire que le concept général des activités des gens qui ont leur propre DNS, ce sont des entreprises qui vont peut-être activer leur propre DNSSEC pour s'assurer que tout est bien géré. Si une activité utilise des sous-traitants pour le DNS, ils vont peut-être aussi pouvoir prendre des sous-traitants pour activer le DNSSEC. Dans

certains cas, les choses deviennent de plus en plus simples. Beaucoup de fournisseurs ont des services externes de DNS qui n'offraient pas dans le passé le DNSSEC. Donc je voudrais insister pour que ces gens-là utilisent des sous-traitants pour qu'ils le fassent. Il n'y a pas beaucoup de gens qui vont le faire mais je sais que si ces personnes ne vont pas trouver de serveurs qui vont le faire, il faut changer d'opérateur pour que ces gens-là mettent en place le DNSSEC.

Il s'agit de ma diapositive qui fait un peu un résumé du DNSSEC. Attendez, revenez en arrière. Nous allons ouvrir la séance pour pouvoir poser des questions et peut-être pouvoir répondre à ces questions. J'espère que vous avez des questions.

DAN YORK : Oui. Si vous voulez bien venir nous poser des questions, nous allons avoir des micros volants pour la salle. Alors, qui donc a des questions ? Il y a des questions, c'est sûr. Il y a Andrew qui va passer dans la salle avec un micro volant. Alors ici, il y a une question. J'avais peur qu'il n'y ait personne ; il aurait fallu qu'on commence à faire des blagues et ça pourrait être difficile. Allez-y.

ROCÍO DE LA FUENTE : Merci pour votre présentation. Je suis Rocío de la Fuente, je suis boursière durant cette réunion. Je voulais juste voir si j'ai bien compris tout cela.

La signature suit la hiérarchie du DNS. Donc si les TLD ne sont pas signés, pour mon domaine, ce domaine qui est enregistré ne peut pas obtenir le DNSSEC ?

DAN YORK : Oui. Non, attendez. Alors, la réponse est celle-ci. Vous pouvez signer votre domaine mais cela ne va pas suivre dans la chaîne de confiance. Quelqu'un ne pourra pas valider jusqu'à la racine. Donc oui, en général, pour que le DNSSEC fonctionne, il faut que le TLD soit signé.

WES HARDAKER : Idéalement, il faut que toute la chaîne soit signée parce que le DNSSEC va vous protéger tout au long de la hiérarchie. La plupart des TLD sont signés maintenant et d'ailleurs, nous allons faire un atelier sur le DNSSEC. Il y a plus de 10 millions de noms de domaine qui sont signés. Je suis sûr que le www.bigbang.com existe et si cela se trouve, il n'est même pas signé. Mais vous devez valider toute la chaîne. Si vous ne pouvez pas valider jusqu'à .com, c'est déjà quelque chose.

DAN YORK : Mercredi, vous pouvez venir à l'atelier de travail et nous allons produire des diagrammes pour vous expliquer tout cela. Vous venez de quel pays madame ? L'Argentine ? Très bien, .ar ? Il va vérifier.

Une autre question dans la salle ?

YAZID AKANHO : Je viens du Bénin et je suis boursier.

Merci pour votre présentation et pour vos diapositives et vos sketchs. Cela nous aide à bien comprendre. Deux questions de ma part.

Tout d'abord, pourquoi déployer le DNSSEC – je ne sais pas exactement quel mot employer ? Le déploiement est très long. Pourquoi est-ce que c'est très long ? Est-ce qu'il y a des raisons techniques, politiques ? Pourquoi est-ce que c'est si lent ?

La deuxième question. On m'a parlé du programme du roadshow DNSSEC. Est-ce qu'il existe toujours ? Quelle est la prochaine étape pour ce programme de roadshow de DNSSEC ?

Et aussi, est-ce qu'on pourrait avoir plus d'explications sur l'infrastructure qui génère les clés pour le DNSSEC ? Est-ce que cette structure doit être maintenue d'une façon ou d'une autre ? Est-ce que vous pouvez expliquer ?

DAN YORK : Le DNSSEC, le roadshow et les informations sur la signature. C'est cela que vous me demandez ?

WARREN KUMARI : J'ai regardé déjà au fait, .ar est signé.

Et quand il s'agit du déploiement, oui, le DNSSEC n'a pas été déployé aussi rapidement qu'on aurait pu. 13,3 % des requêtes sont validées par exemple au Canada, 25 % aux États-Unis, 90 % au Groenland et

14 % en Russie. Donc ce n'est pas si déployé que cela. Mais le déploiement augmente, et la plupart des demandes sont validées et la plupart des TLD sont signés. Et les nouveaux contrats des TLD fournissent ces informations. La plupart des ccTLD aussi sont signés.

WES HARDAKER : Si vous voulez suivre les choses de façon journalière, mon collègue Victor et moi avons un site web que nous actualisons de jour en jour. Cela s'appelle stats.dnssec-tools.org. Si vous regarder le diagramme, vous allez voir que le déploiement a augmenté depuis 2011. Des fois, il y a de grands soubresauts de déploiement. Il y en a eu il n'y a pas très long d'ailleurs parce que one.com, qui est un fournisseur, a signé beaucoup de choses sous le .dk, donc il y a eu une grosse augmentation.

On a besoin de plus de choses comme cela, on a besoin de grosses entreprises qui le fassent par défaut. La plupart des domaines qui sont utilisés dans le monde sont utilisés par des grosses entreprises. Et de façon traditionnelle, il y a eu des gros soubresauts au niveau du déploiement. Par exemple, en République tchèque, il y a eu des incitatifs pour le déploiement. Ainsi, les enregistrements sont moins chers et cela permet de faire une poussée justement pour qu'il y ait plus de déploiement, plus d'entreprises qui signent.

RUSS MUNDY : Il y a beaucoup d'incitatifs différents qui ont été utilisés par des organisations variées pour encourager les gens à faire le DNSSEC. Et

dans ce sens, il y a quelque chose qui a beaucoup aidé, c'est que la plus grande partie de tout les résolveurs publics qui étaient disponibles, la plupart d'entre eux emploient maintenant la validation du DNSSEC.

Une des choses sur lesquelles nous avons travaillé d'ailleurs et depuis longtemps, c'est que nous voulions voir justement cette validation, que cette validation aille jusqu'à l'application finale. Il y a des exemples qui ont été utilisés dans cette présentation. On a parlé tout à l'heure du piratage avec la page qui parlait de Steve Crocker. Cette attaque avait été produite au niveau du moteur de recherche. Il faut continuer à voir que quand les validations sont faites jusqu'à la fin, donc vers l'utilisateur, le mieux c'est. Donc il faut encourager les gens à le faire, surtout les résolveurs publics les plus importants aussi. Pensez aux applications aussi. Il y avait une autre question.

DAN YORK : Et par rapport à cela, le problème de déploiement, c'est que comme ce que vous voyez à l'écran, en fait, il y a deux parties. Toutes les personnes qui signent, qui ont un domaine, doivent signer ; donc cela, c'est la première partie, c'est la partie signature.

Maintenant, Russ l'a dit, cela peut être automatisé en partie, nous avons des outils qui existent et vous allez parler à des hébergeurs de DNS, vous savez qu'ils peuvent faire cela de manière très facile. Il y a des gens qui simplement vous demandez de cocher, vous terminez et vous êtes signé. Donc c'est assez facile mais le problème, c'est qu'il faut vérifier, il faut valider. Et come Russ l'a dit, parfois, c'est

simplement de décocher, d'éliminer une ligne de commentaires dans un fichier de configuration et là, vous allez valider.

Mais pendant longtemps, ce qui s'est passé, c'était un petit peu la question de la poule et de l'œuf comme on dit souvent aux États-Unis. Certains des opérateurs de réseau, certains des FSI comme Warren le montrait, n'utilisaient pas la validation. Ils disaient : « Nous n'allons pas mettre en marche la validation parce qu'il n'y a pas suffisamment de domaines signés. » Alors, les opérateurs disaient : « Oui, il n'y a pas suffisamment de domaines signés et les grands hébergeurs disaient : « On ne va pas signer nos domaines parce que nous n'avons pas suffisamment de personnes qui valident. » Donc c'était un cercle vicieux.

Maintenant, nous avons dépassé en grande partie ces obstacles parce que comme Russ la dit, il y a davantage de déploiement, il y a des gens qui ont une résolution récursive. Par exemple le DNS public de Google, Cloudflare, eux, tous, ils effectuent la validation de DNSSEC. Donc il y a de grands FSI qui le font, Comcast en Amérique du Nord avec les 20 millions de clients qu'ils ont font la validation.

Donc cet argument comme quoi la validation aurait ralenti le déploiement, il existe toujours mais il n'est plus vraiment justifié.

Vous aviez un commentaire ?

FRED BAKER : Je voulais poser une question à Russ. Est-ce que vous connaissez des navigateurs spécifiques qui soutiennent la validation du DNSSEC ?

Moi, je n'ai que quatre navigateurs sur mon ordinateur. Qu'est-ce qu'il faut que j'utilise ?

RUSS MUNDY : Alors, malheureusement, il n'y a pas de navigateur qui ait une validation intégrée du DNSSEC. Nous en avions un, nous l'avions utilisé pendant un moment, mais cela ne fonctionne plus.

WARREN KUMARI : C'est la validation DANE dont on parle. Ce n'est pas cela ?

Les navigateurs utilisent le résolveur de système. Si votre ordinateur effectue la validation DNSSEC, les navigateurs utilisent le résolveur du système. Donc si vous avez activé la validation du DNSSEC sur votre ordinateur, vous avez la validation du DNSSEC gratuitement. Wes va maintenant me gronder.

WES HARDAKER : Non, je ne me permettrais pas.

FRED BAKER : Donc sur mon Mac, sur mon Windows, sur ma machine Linux, il faut que j'aille faire quelque chose. C'est cela ? C'est ce que vous êtes en train de me dire ?

WES HARDAKER : En fait, on va rentrer vraiment dans les questions très techniques et très difficiles à décrire, mais il y a certains éléments pour lesquels on peut faire la validation. Donc de nos jours, les applications – donc les navigateurs, les lecteurs de courriels, etc. tout ce qui accède au réseau, c'est choses-là ne font pas la validation en elles-mêmes. Comme dans le sketch, je n'ai pas vérifié moi-même, j'ai fait confiance à mon FSI qui l'a fait pour moi.

FRED BAKER : En tant qu'utilisateur, Joe est une personne terrible.

WES HARDAKER : Je suis un utilisateur terrible effectivement. Donc j'ai les codes de validation et il y a des paquets IP dont on parlait tout à l'heure qui ont des codes de validation dans le paquet open source et qui vérifient dans l'application. Il y a très peu d'applications qui le font. Il y en a une, une des plus grosse, si vous allez voir les statistiques dont on parlait tout à l'heure.

Une des plus grandes motivations pour le déploiement de nos jours, c'est que c'est un des seuls moyens, un des meilleurs moyens de sécuriser les courriels entre serveurs. Cela accélère assez rapidement. Ce n'est pas tout le DNSSEC mais si vous regardez un petit peu la technologie DANE qui signe les courriels, c'est vraiment une technologie qui grandit le plus.

WES HARDAKER : Vous avez dit en tant qu'utilisateur que vous deviez faire quelque chose. En tant qu'utilisateur, vous deviez vous assurer que votre FSI valide les résolveurs. Vous pouvez leur poser la question ou alors vous pouvez choisir un des grands résolveurs publics, 111199998888 par exemple, parce qu'ils font tous la validation. Donc si vous voulez la protection DNSSEC, d'abord demandez au FSI s'il valide, sinon utilisez un autre résolveur. Il y a un site internet qui permet de vérifier si les résolveurs actuels que vous utilisez effectuent la validation. Comme cela, vous pourrez savoir si votre FSI l'effectue.

DAN YORK : Fred, en ce qui concerne les navigateurs, on reporte certaines questions à mercredi. Mais il y a aussi le DoH, il y a certains navigateurs qui font ceci, il y a des endpoints qui sont des serveurs DoH qui font également la validation DNSSEC. Donc votre navigateur le fait peut-être. Mais bon, ne passons pas à DoH maintenant, revenons à la question de Yazid parce qu'il est très patient là-bas. Je suis désolé, je ne sais pas si j'ai bien prononcé votre nom.

YAZID AKANHO : Mon nom est Yazid.

Merci d'avoir clarifié la question de la validation des résolveurs et la question de la signature de la zone, qui sont en fait deux aspects séparés si je comprends bien.

Il y a deux ans, dans mon pays le Bénin, on a été surpris lorsqu'on s'est rendus compte que 80 % des requêtes étaient validées DNSSEC par les

résolveurs. Pourquoi ? Parce que certains FSI utilisaient des résolveurs publics. Donc c'est complètement différent de la signature de la zone. Donc voilà pourquoi je posais la question de savoir où se trouvait cette tournée DNSSEC, ce roadshow DNSSEC.

DAN YORK : Oui, vous avez tout à fait raison. Et par rapport aux statistiques, je sais qu'il y a certains pays qui ont de hauts niveaux de validation DNSSEC. Et en fait lorsqu'on regarde le détail, on se rend compte que certains des FSI de ces pays utilisent des résolveurs publics et n'utilisent pas leur propre résolveur et utilisent 8.8.8, etc., un des résolveurs publics qui existent.

En ce qui concerne la tournée DNSSEC de l'ICANN, je ne sais pas. Nous ne sommes pas impliqués dans ce programme directement, donc il va falloir qu'on réponde à votre question plus tard. Yazid, n'hésitez pas à nous contacter, à nous donner vos coordonnées.

En ce qui concerne la documentation, je peux également entrer en contact avec vous. L'Internet Society a publié des informations, il y a également l'ICANN qui a publié des informations. Il y a plusieurs ressources qui existent et qui parlent des détails. Beaucoup des sociétés de résolveurs faisant autorité, l'Internet Lab, etc. ont créé leurs propres documents là-dessus. Donc il y a des liens qui sont utiles.

D'autres questions ? Oui, monsieur.

ORATEUR NON-IDENTIFIÉ : Merci. Je ne sais pas si cela rentre vraiment dans le sujet. Je voulais savoir quel est le lien entre le DNSSEC et le sig zéro et la réponse sig.

WES HARDAKER : Il n'y a pas de lien. Le DNSSEC est mis en place pour protéger un ensemble de données et les rendre vérifiables de manière à ce que vous compreniez les données lorsqu'elles vous arrivent. Là, ce que vous avez mentionné, c'est une autre technologie qui sécurise les connexions, pas les données en elles-mêmes, quel que soit le cheminent qui est pris. En fait, ce sont des technologies complètement différentes.

WARREN KUMARI : Pour faire un suivi là-dessus, Wes a dit que DNSSEC vous permet de valider les informations quelque soit le chemin qu'elles prennent pour vous arriver. Une des choses que l'on peut ajouter par rapport à cela, c'est qu'il y a un certain nombre de personnes qui téléchargent actuellement toute la zone racine dans le résolveur parce que tout est signé. Donc vous pouvez simplement valider avec votre résolveur et vous n'avez pas besoin d'envoyer la même requête. Cela, c'est un des aspects positifs d'une zone signée, vous pouvez simplement laisser quelqu'un d'autre faire le travail.

ORATEUR NON-IDENTIFIÉ : Par rapport aux requêtes de transfert, comment est-ce qu'on a tout le fichier de zone ?

WARREN KUMARI : Beaucoup des acteurs B et F et d'autres vous laissent faire une requête AXFR. Si davantage d'informations vous intéressent, vous pouvez regarder local root.

DAN YORK : Ou hyperlocal root.

WARREN KUMARI : Il y a un projet qui vous permet de le faire sur une page web.

WES HARDAKER : Oui. Je peux vous renvoyer sur localroot.isi.edu et vous avez un résolveur avec un cache. Donc c'est utile si vous êtes administrateur et si vous avez certaines connaissances.

ORATEUR NON-IDENTIFIÉ : Autre question sur le DNSSEC. Par exemple si vous avez le .com, vous avez des dizaines de serveurs de noms. Est-ce que chacun a une clé DNSSEC unique pour chaque machine et est-ce que c'est une clé pour tout le TLD ?

WARREN KUMARI : Vous signez en fait une zone. Donc une fois que la zone est signée, vous pouvez la mettre sur n'importe quel serveur de noms. Donc c'est vraiment pratique si vous avez votre propre serveur de noms et si vous

avez une autre organisation qui est en fait esclave ou secondaire. Vous signez votre zone, vous lui donnez la zone, il n'y a pas d'autre clé, donc pas besoin de s'inquiéter de ces personnes.

DAN YORK : C'est cela la beauté du fonctionnement. Une fois que vous avez tout signé, vous pouvez simplement la communiquer. C'est la clé publique, la clé privée.

D'autres questions ? Ce peut être des questions génériques, ce peut être des questions stupides, ce peut être « Pourquoi est-ce que le DNSSEC ont le SEC à la fin ? », « Qu'est-ce que cela veut dire ? » Oui, Yazid.

YAZID AKANHO : Autre question.

J'ai entendu dire qu'il y a des investigations ou des analyses qui viseraient à changer le protocole qui génère les clés publiques et privées de la zone racine. Où ont lieu ces discussions et que nous réserve l'avenir ?

DAN YORK : Je pense que mes collègues qui sont là pourraient peut-être en parler, mais vous avez raison. Lorsqu'il y a la signature, vous voyez en haut pour le premier serveur, vous signez grâce à un algorithme cryptographique. Cela peut être une courbe elliptique, cela peut être autre chose, mais ces algorithmes cryptographiques ont différentes

propriétés. Certains sont plus ou moins sécurisés, les protocoles d'origine ont déjà été compris. Donc maintenant, on doit passer à un niveau de sécurisation supérieur. On considère plutôt les courbes elliptiques qui sont plus courtes aussi. Donc oui, il y a différents algorithmes qui existent.

En ce qui concerne la racine, Warren, vous voulez dire quelque chose ?

WARREN KUMARI : Je vais faire un commentaire d'ordre général.

DAN YORK : Vous avez poussé le bouton, je l'ai vu, vous vouliez prendre la parole.

WARREN KUMARI : D'accord. Alors, il y a pas mal de croyances par rapport aux meilleur protocole cryptographique. Donc en général, les gens ne sont jamais d'accord, ils s'attaquent là-dessus, est-ce que le RSA est meilleur, est-ce que c'est le ED 25519 qui est meilleur, etc. ; beaucoup de débats.

Pour l'instant, il y a eu une migration de RSA à certains protocoles mais certaines personnes commencent à parler des protocoles sécurisés quantum secure. Certains ordinateurs, apparemment, pourraient avoir un impact sur le fonctionnement de ces protocoles. Donc c'est un petit peu ce que les gens commencent à voir et le sujet des débats.

DAN YORK : Je crois que du côté de la racine, il n'y a pas de plan immédiat pour changer le protocole. Russ ?

RUSS MUNDY : Nous n'allons pas le changer mais je voudrais quand même promouvoir ou plutôt faire la page pub pour notre atelier de mercredi parce que nous allons justement avoir une présentation de Kim Davies sur ce qui est prévu pour le prochain roulement de KSK de la racine. Donc si vous êtes intéressé par davantage d'informations, par des détails sur quand, comment, également sur les différents commentaires de la communauté par rapport à cela, vous avez un atelier sur le DNSSEC l'après-midi, je crois que c'est une séance de 20 à 25 minutes pendant laquelle Kim, qui est président de la PTI qui gère l'IANA, fera une présentation sur le premier jet du plan qui vient en fait d'être publié vendredi ou samedi.

DAN YORK : Et cet atelier sera à 13:30 à côté dans la salle 517C. Donc il y aura plusieurs heures passées à discuter de différentes questions relatives au DNSSEC. Certaines des questions sont vraiment de très haut niveau, d'autres sont vraiment basiques, donc il y a un petit peu de tout. Vous verrez, on y sera.

Y a-t-il d'autres questions ? Andrew est là, il a levé la main, il faudrait peut-être l'aider. Personne ? Les conseils sont gratuits. Sinon, on va recommencer à faire des blagues. Regardez un petit peu, c'est parfait. J'ai utilisé ma menace de la blague et cela a marché.

ORATEUR NON-IDENTIFIÉ : Je ne sais pas, c'est peut-être une question bête mais je voulais clarifier quelque chose. C'est en fait un suivi à la question de Fred de tout à l'heure. En fait, si je n'ai pas un navigateur qui est compatible avec le DNSSEC, Outlook ou que sais-je, donc est-ce que cela veut dire que la partie qui est entre mon résolveur DNS et mon client n'est pas protégée techniquement ?

DAN YORK : Oui, mais il faut que je clarifie quelque chose. Toutes les applications de votre dispositif historiquement ont toujours laissé la résolution du DNS à un résolveur stub dans le système opérationnel qui ensuite envoyait les requêtes au FSI, etc.

Donc si votre système d'exploitation n'était pas compatible avec la vérification des signatures, et bien oui, vous étiez en situation de risque et le diable pouvait venir prendre les informations et vous diriger vers un autre site. Donc c'est ce qui s'est passé du point de vue historique, en dehors des exemples où les gens avaient mis en place une validation DNSSEC par eux-mêmes.

Mais ceci évolue. Il y a tout un groupe au sein de l'IETF qui essaie de voir un petit peu ce qui se passe au niveau des applications qui font le DNSSEC. Vous avez le DoH, vous avez les navigateurs web, etc. mais il y a d'autres applications qui travaillent davantage sur la validation des DNSSEC et qui changent un petit peu l'architecture du fonctionnement du DNS et du fonctionnement de l'internet.

Warren veut dire quelque chose ?

WARREN KUMARI : Oui. Warren pense que nous avons trop vendu la protection en fait. Ce qui se passe, c'est que si le FSI fait toute la validation et si le FSI revient vers l'internaute et dit : « Oui, ne t'inquiète pas, j'ai tout validé. » en fait, le DNSSEC ne fonctionne pas exactement comme cela. Il y a un résolveur de validation, un FSI etc. qui fait le DNSSEC et il dit au client qu'il peut faire confiance : « Tout va bien, ne vous inquiétez pas. » Donc cela veut dire que si le paquet, en revenant du résolveur au client est impacté, il peut y avoir un problème.

Donc certains systèmes d'exploitation sont forcés à le faire, par exemple Linux. Vous pouvez mettre en marche ou éteindre et la validation se fait d'elle-même. Donc les gens fournissent un logiciel, par exemple il y a le stubby qui fait la validation sur l'ordinateur. Mais d'une manière générale, vous faites confiance au FSI et vous imaginez qu'il a fait le boulot pour vous et vous faites confiance à votre FSI et pensez qu'il ne manipule pas les données.

ORATEUR NON-IDENTIFIÉ : Je pensais que si vous aviez quelqu'un sur votre réseau local qui empoisonne et qui répond aux requêtes plus rapidement, c'est à cela que je pensais.

DAN YORK : Oui, c'est le genre d'attaque qui peut se produire. C'est pour cela qu'on voit beaucoup de travail qui est fait au niveau de la vie privée et du DNS. Il y a du travail du groupe en ce moment qui discute du chiffrement des connexions pour ainsi pouvoir avoir une connexion qui soit sûre et pour que les réseaux locaux ne peuvent pas avoir un impact. Ce sont des couches et des couches de protection du DNS.

WARREN KUMARI : Il y a deux genres d'attaque. Il y a quelqu'un sur votre réseau qui empoisonne et qui vous donne les mauvaises réponses et qui vous force à aller aux mauvais endroits. Mais il y a aussi quelque chose qui menace énormément. Il y a quelqu'un sur le réseau qui observent vos paquets et cela dépasse si vous avez https://alcooliquesanonymes.org, le contenu est chiffré donc on peut vous envoyer au mauvais endroit, surtout pour ces sites dans ce genre. Le fait que vous avez les résolveurs pour certains noms qui sont chiffrés, cela peut causer beaucoup de dommages.

RUSS MUNDY : Comme Warren le disait, il arrive qu'il y ait des choses qu'on appelle l'attaque du café, *coffee shop attack*. Leur wifi est peut-être encrypté mais pour d'autres, c'est accessible. Donc pour toutes les personnes qui sont dans ce même café peuvent rejoindre le même wiki et ensuite peuvent ainsi faire des copies ou même donner des fausses réponses à vos requêtes DNS. Donc si vous, vous avez une manière de vous protéger ou de protéger votre machine et ainsi pouvoir aller au bon endroit et avoir des informations exactes, vous serez ainsi moins

vulnérable aux attaques. Je sais pour ma part que c'est une chose qui est totalement faisable. Il y a des logiciels qui sont disponibles sur l'internet qui vous permettront de faire cela.

DAN YORK : Le DNSSEC est là pour vous assurer d'avoir la bonne réponse. Ce dont on parle ici, ce sont des couches supplémentaires pour la vie privée. On en parlera d'ailleurs durant l'atelier mercredi ; on va parler de tous ces éléments. Ça va ? Cela répond à votre question ?

ORATEUR NON-IDENTIFIÉ : Oui, cela répond à ma question.

DAN YORK : Est-ce qu'il y a quelqu'un qui pose une question sur l'internet ?

KATHY SCHNITT : « Est-ce que vous pouvez nous parler de ce qui se passe avec Firefox ? »

DAN YORK : Alors, le DoH. Je ne sais pas exactement si on devrait rentrer dans les détails ici. Est-ce qu'il y a des points de vue ?

WES HARDAKER : C'est moi qui ai donné la réponse lorsque cette conversation a eu lieu auparavant. Mais attendez, je vais revenir en arrière. Je vais répondre à la question qui a été posée tout à l'heure.

Il y a de multiples manières de protéger la conversation entre vous et le résolveur. On étudie toujours la question. Il y a un groupe de travail de l'internet qui travaille là-dessus. Vous pouvez faire quelque chose comme DoH, DoT. Il y a des tas de manières pour pouvoir vous protéger. Tous ces systèmes fonctionnement.

Quand il s'agit des navigateurs web, ils ont déjà décidé car ils sont experts et ils comprennent le protocole, ils savent l'utiliser, ils savent faire les choses, ils ont déjà décidé qu'ils veulent faire DNS sur HTTPS. Je ne connais pas tous les plans. Je sais qu'il y a un plan différent pour Chrome et Firefox.

Firefox l'a annoncé au début ; ils ont dit qu'ils allaient collaborer avec Cloudflare. Cloudflare est une compagnie qui a des tas d'éléments et ils comprennent très bien les résolveurs de validation DNSSEC dans le monde. Ils vont donc collaborer avec Cloudflare pour envoyer toutes leurs requêtes DNS. Si vous utilisez donc Firefox et que vous êtes aux États-Unis, les plans de déploiement ne sont pas encore mis sur le calendrier mais je pense qu'il va y avoir un test aux États-Unis ce mois-ci avec Cloudflare. Vous aurez une liste de toute façon et vous pourrez choisir votre fournisseur.

Pour Google par contre – et Warren va me corriger si ce n'est pas vrai – Google va donc essayer de tester votre FSI pour voir si votre FSO fournit HTTP ou HTTPS pour le DNS. Et s'ils le font et qu'ils sont sur la

liste de confiance, ils vont utiliser DoH pour conversera avec votre FSI. Et si cela ne fonctionne pas, ils reviendront au DNS régulier. Ils ne vont pas envoyer tout cela vers une tierce partie par contre.

WARREN KUMARI : Oui. En fait, tout cela est très correct. Il y a une chose que je voulais rajouter par contre.

L'approche de Chrome est celle-ci. Google dit qu'il devrait continuer avec le résolveur courant parce qu'il se préoccupe ainsi de la protection, vos résolveurs ne doivent pas changer. Votre résolveur va vous permettre une protection vis-à-vis des noms de domaine généraux ; c'est l'approche Google.

DAN YORK : Il est important de comprendre aussi qu'il y a un protocole qui s'appelle DoH, DNS sur HTTPS. C'est un protocole qui explique comment faire le DNS par une connexion HTTPS. Il y a donc un protocole DoH qui peut converser avec tous les serveurs DoH. Il y a donc une connexion cryptée et sécurisée entre l'application et le résolveur DNSSEC. Donc le protocole DoH, c'est cela. Alors qu'il est déployé à l'état précoce, on rencontre ces problèmes parce que justement, il y a des problèmes de connexion. Il est donc important de savoir qu'il y a un protocole qui se préoccupe de cette couche de sécurité pour s'assurer justement comme on le disait tout à l'heure que toutes les personnes qui sont dans un café par exemple qui sont sur un même wiki n'aient pas de problème.

Il y a DoT qui est un autre protocole est qui est conçu pour protéger la vie privée. Ils augmentent le niveau de confidentialité. Et le problème, c'est comment ces systèmes doivent être déployés au début.

WARREN KUMARI : Wes a parlé de cela tout à l'heure. Je travaille pour Google qui utilise Chrome.

RUSS MUNDY : Pour les personnes qui veulent en apprendre un peu plus sur ce sujet, lors de l'ICANN64, il y avait eu une séance de deux heures sur les sujets brûlants justement à propos du DoH, et DoT avait été mentionnée. C'était une séance qui a durée très longtemps. Elle est enregistrée et je suis à peu près sûr qu'elle est disponible dans les archives sur le site web pour l'ICANN64. Vous pouvez y aller et vous pouvez voir, écouter cette discussion sur l'internet.

ANDREW MCCONACHIE : Je pense que c'était l'ICANN65. Il y a eu une séance à Marrakech sur le DoH. N'est-ce pas ?

WES HARDAKER : Oui. Je travaille à l'université de la Californie du Sud.

WARREN KUMARI : Je pense qu'il doit y avoir encore plus d'informations. Je n'ai pas encore vérifié.

WES HARDAKER : Je pense qu'on a une séance sur le DoH aussi mercredi.

DAN YORK : Y a-t-il d'autres questions dans la salle ? Oui, monsieur devant.

ORATEUR NON-IDENTIFIÉ : Je suis un type qui vient des États-Unis.

Comment est-ce qu'on peut faire les requêtes au niveau privé qui ne sont pas ce qu'on appelle les requêtes coffee shop dans le cas où la demande est encryptée ?

DAN YORK : Oui. Ces technologies vous permettent de faire cela ; on parlait de DoH et de DoT. Vous pouvez faire cela à partir de votre navigateur si vous êtes sur Chrome ou sur Firefox. Vous pouvez les installer maintenant pur utiliser DoH et vous pouvez leur dire vers quel serveur ils doivent se connecter. Vous pouvez donc le faire maintenant. Vous pouvez aller aussi à dnsprivacy.org. Il y a des tas de logiciels que vous pouvez utiliser. Il y a aussi un logiciel qui s'appelle stubby. Vous pouvez envoyer toutes vos requêtes vers un serveur DoH. Vous pouvez aussi faire votre propre serveur DoT ou DoH. Vous pouvez le faire vous-même et installer cela vous-même.

WARREN KUMARI : Et vous pouvez aussi démarrer le VPN si vous avez des problèmes.

DAN YORK : Y a-t-il d'autres questions dans la salle ?

ROCIO DE LA FUENTE : Quand il s'agit de la visibilité numérique, quand on parle de l'éducation vis-à-vis des utilisateurs ou des titulaires de nom de domaine, est-ce qu'on doit leur expliquer l'importance qu'a le DNSSEC pour leur domaine lorsqu'ils s'enregistrent ? Parce qu'on a parlé des FSI, des opérateurs et des bureaux d'enregistrement. Oui, je parlais des opérateurs de registre. Mais lorsque l'on parle de cela, est-ce que cela pourrait aider le déploiement du DNSSEC ? Quelle est votre opinion sur ce sujet ?

DAN YORK : Je peux vous répondre. Je peux vous dire oui, absolument, nous encourageons les gens à inclure cela. Quand on déploie son domaine, il doit être signé. Encore une fois, certains des bureaux d'enregistrement, je ne sais pas ce qui se passe en Argentine pour vous, mais il y a encore une fois des bureaux d'enregistrement qui sont arrivés à un point où ils font les choses d'une façon très facile ; c'est devenu une procédure simple et cela, c'est idéal et c'est là où on veut en arriver quand il s'agit de la signature. Il faudrait que ce soit quelque chose de simple, quelque chose qui n'implique pas grand-chose de la part de l'utilisateur final. Nous voulons que les gens s'impliquent et que les gens signent. Nous pensons qu'au niveau de la réputation, cela permet aux personnes d'arriver sur les sites qu'ils recherchent.

WARREN KUMARI : Est-ce que je peux être en désaccord un peu ? Donc, je ne suis pas forcément d'accord, cela dépend du point où on en est. On peut vous dire que le DNSSEC c'est une bonne chose, mais est-ce que c'est la chose la plus importante pour un nouvel utilisateur de l'internet ? Probablement que non. Est-ce que c'est la chose la plus importante quand quelqu'un enregistre un domaine ? Oui, ce pourrait l'être. Il y a d'autres choses quand il s'agit de la sécurité. Donc de cette manière là, oui et non.

DAN YORK : Oui Warren, merci pour votre réponse.

WARREN KUMARI : Je pensais à cela aussi, quand on pense aux incitatifs, par exemple nous nous impliquons à l'ICANN et à la gouvernance de l'internet mais si on n'a pas un historique technique, on doit passer énormément de temps et d'efforts pour essayer de comprendre pourquoi le DNSSEC est important. Donc les utilisateurs ou les bureaux d'enregistrement qui y pensent, comment est-ce qu'ils peuvent essayer de mettre en place un récit ou pouvoir expliquer la raison pour laquelle un domaine peut être un peu plus cher, mais ce domaine est sécurisé ?

DAN YORK : Cela fait partie du défi. Dans beaucoup d'endroits, nous avons travaillé avec le DNS, avec les fournisseurs d'hôtes, les fournisseurs de

DNS et les bureaux d'enregistrement pour les encourager justement à ce que cela se produise. Et certains le font et signent par défaut. Il faut essayer de faciliter les choses pour que les gens puissent le faire. Bien sûr, cela coûte de l'argent. Et je suis d'accord avec Warren parce qu'en général, quand quelqu'un va en ligne, c'est quelque chose de plus à faire. Mais tout cela dépend de leur niveau d'expertise. Ce n'est pas forcément une priorité pour tout le monde et pour cela, c'est quelque chose que l'on va observer au niveau de l'infrastructure.

Y a-t-il d'autres questions ? Nous avons le temps pour une question ou deux. Non, il n'y a pas de questions ? Monsieur Levine, ici, vous avez une question ? Je dis cela parce que je connais ce monsieur très bien.

JOHN LEVINE : C'est une publicité en fait.

Il y a un moment, vous avez parlé de la cryptographie quantum et de son impact sur le DNSSEC. Je pense qu'on va en parler durant la journée technique demain. La personne qui va faire la présentation n'est pas géniale mais bon, on ne peut rien y faire.

WES HARDAKER : Nous assumons que vous allez faire cette présentation.

DAN YORK : John va donc faire une présentation là-dessus demain. Si vous êtes nouveau, d'ailleurs demain, c'est la journée technique. Il y a beaucoup de réunions qui auront lieu dans ces salles et il y a beaucoup de sujets

qui seront discutés. On va parler de la cryptographie quantum et tout autre chose dans ce genre. Je n'ai pas regardé encore l'ordre du jour pour cette semaine donc je ne suis pas tout à fait au courant.

WARREN KUMARI : Cette réunion aura lieu dans la salle 517C.

DAN YORK : Et cela commence à 10:30 demain matin.

Y a-t-il autre chose ? Très bien. Donc si c'est tout, je voudrais vous remercier de votre présence. Si vous êtes intéressé à notre travail, vous pouvez venir nous voir ici et nous pouvons répondre à vos questions. Encore, salle 517C ce mercredi, nous allons avoir l'atelier de travail sur le DNSSEC. Vous pouvez aller sur l'ordre du jour et voir un petit peu quel sera notre agenda pour cette séance.

Passez une bonne semaine à l'ICANN.

[FIN DE LA TRANSCRIPTION]