SAN JUAN – DNSSEC pour tous : un guide du débutant
Dimanche 11 mars 2018 – 17h00 à 18h15 AST
ICANN61 – San Juan, Porto Rico

WES HARDAKER : Bon. Bienvenue à tous. Vous êtes à la présentation sur le DNSSEC pour les débutants. Donc c'est un guide DNSSEC. Donc même si vous ne connaissez pas beaucoup, vous n'avez pas beaucoup de notions techniques, nous espérons que vous aurez les bases relatives à la structure DNSSEC. Ça va à l'arrière ? Vous m'entendez ? Oui ? Très bien.

Alors nous allons donc parler des DNSSEC et comment cela fonctionne et nous allons commencer par le début. Nous allons même commencer par les tous débuts, la préhistoire, donc aux origines, 5000 av. J.-C. On va essayer d'agrandir un petit peu les diapositives, s'il vous plaît ? Merci mais je continue pour l'instant.

Donc je vais vous raconter une petite histoire. C'est l'histoire d'Ugwina. Ugwina habite dans une grotte aux portes du Grand Canyon. Je vous promets que vous allez comprendre à quoi cela correspond. Et j'ai perdu le contrôle des diapositives. Ça y est. Merci beaucoup. J'espère que vous voyez mieux. Donc voilà, vous avez Og, homme magnifique qui habite dans une grotte de

l'autre côté du Grand Canyon. Et donc pour se rendre de l'autre côté, c'est vraiment très très long. Ugwina et Og s'entendent très bien mais ils n'arrivent pas beaucoup à communiquer parce que c'est vraiment difficile d'aller d'un endroit à l'autre.

Donc de temps à autre, ils se voient et tout d'un coup, ils se disent : « Tiens, il y a de la fumée qui sort de ce feu. » Et donc ils se disent, tiens, on pourrait communiquer en utilisant des signaux de fumée. Jusqu'à ce qu'un jour, le méchant homme des cavernes Kaminsky qui a fait, je crois, une attaque du DNS en 2008, n'est-ce pas ?

Donc Kaminsky arrive et il s'installe à côté de chez Og et commence à envoyer des signaux de fumée. Et la pauvre Ugwina de l'autre côté du Grand Canyon n'y comprend plus rien. Elle ne sait plus à quelle fumée se vouer. Donc Ugwina descend dans le Grand Canyon pour essayer de comprendre un petit peu ce qui se passe. Ugwina et Og parlent au sage du village, Diffie Hellman qui a créé une forme de cryptographique qui est utilisée dans le DNSSEC, donc c'est de là que ça vient – donc l'homme des cavernes Diffie pense avoir une bonne idée. Il se dépêche de courir pour se rendre dans la grotte de Og et à l'arrière, il voit une pile de sable d'une étrange couleur que l'on ne trouve que dans la grotte de Og. Il se dépêche et il jette du sable sur le feu et tout d'un coup, la fumée devient d'un bleu magnifique.

Donc Ugwina et Og peuvent maintenant discuter tranquillement en sachant que personne ne peut intervenir dans leurs conversations. Donc voilà, c'est magique, on sait tout de suite quand les gens envoient un faux signal ; c'est très important pour la suite. Donc voilà pour la petite présentation rapide des DNSSEC et comment cela fonctionne.

Nous allons maintenant rentrer dans le détail. Et je travaille pour l'université d Californie du Sud, ISI. Dan York est en principe la personne qui s'occupe de cette présentation mais il n'est pas là. Donc désolé, vous n'avez que moi. Russ sera avec moi tout à l'heure.

Et à la fin de la journée, vous allez pouvoir poser des questions. Donc au fil de la journée, si vous avez des questions, n'hésitez pas à les noter et on pourra y reporter. Nous avons toute une pléthore d'experts DNSSEC qui pourront répondre à vos questions également.

Alors parlons maintenant du concept de haut niveau par rapport au DNS. J'imagine que pour la plupart d'entre vous, vous connaissez le fonctionnement du DNS, au moins les bases. Mais nous allons quand même en parler un petit peu.

Le DNS, c'est un petit peu comme un arbre. Et donc la zone racine, vous savez où elle se trouve, donc il y a tout un processus dans la hiérarchie. Chaque niveau renvoie le résolveur au niveau

suivant jusqu'à ce que la question ait eu une réponse. Donc en fait, le résolveur passe dans tout l'arbre jusqu'à ce qu'il puisse répondre à la question.

Alors ce qui est important, c'est que le résolveur cache ces informations pour l'avenir. Donc si vous revenez au www.icann.org une seconde après, le résolveur se souvient des informations précédentes de votre première recherche, donc il n'a pas à passer par tout l'arbre. Mais ce qui est important, c'est qu'au départ, il n'y avait pas de sécurité dans le DNS. Donc c'est un petit peu comme les signaux de fumée. Vous avez deux réponses de deux personnes et vous vous dites : « Je ne sais pas laquelle croire. » ; on ne sait pas laquelle est la bonne.

Donc il était très facile d'usurper des noms et une fois que c'est dans le cache, les fausses informations, lorsque quelqu'un a empoisonné votre cache pour icaan.org, et bien pendant très longtemps en fait, vous retournez à ces fausses informations

Donc étant donné la petite histoire sympathique de tout à l'heure, c'était très sympathique, n'est-ce pas ? Mais je vais donc passer à un petit sketch. Est-ce que vous avez déjà regardé ce sketch ? Et pourquoi est-ce que vous êtes là ? Est-ce que c'et pour encore une fois vous moquer de nous quand on fait notre super sketch ? C'est bien ce que je croyais.

Alors j'ai des supers acteurs qui sont avec moi et donc nous allons un petit peu imiter le fonctionnement du DNS. Donc on va vous montrer un petit peu sur la base d'un diagramme comment cela fonctionne. Alors j'ai quelques participants.

J'ai Cathy qui sera la racine du DNS. Donc c'est vraiment le plus haut niveau de l'arbre. Donc c'est le directeur. Vous pouvez décider, comme vous voulez, allez-y. Mettez-vous là. Je vais d'abord vous présenter. Donc voilà le .com. Lui, il sait où toutes les choses relatives au .com se trouvent. Et là, c'est Ross, c'est Big Bank. Donc la grande banque. Donc moi, je suis un utilisateur.

Alor je vais à ma banque, je m'assis à l'ordinateur en fait, je tape et je me dis : « Je vais regarder où j'en suis, quel est mon solde en banque. » Donc j'appuie sur www.bigbank.com et mon navigateur va faire mon résolveur va qui se trouve chez mon FSI. Alors on a même des exemples, regardez. C'est bon, c'est cela... c'est cela. Désolé, on est arrivés à la dernière minute et on ne s'est pas bien organisés. Alors je vais m'adresser à mon FSI. Je lui dis : « J'aimerais bien savoir où est le www.bigbank.com. J'aimerais connaître mon solde en banque. »

ORATEUR NON-IDENTIFIÉ : Bonjour Joe. J'ai votre requête. Vous voulez aller chez bigbank.com mais moi, je suis résolveur de FSI et donc je ne suis pas très au courant de tout cela. Donc je vais essayer de

m'informer. Donc je vais d'abord me rendre dans la racine, je vais poser la question à la racine : « Est-ce que vous savez où se trouve le www.bigbank.com ? »

CATHY : Non, désolée. Mais je sais où se trouve le .com : 1.1.1.1. Voilà où est le .com.

ORATEUR NON-IDENTIFIÉ : Très bien, merci. .com, est-ce que vous savez où se trouve le www.bigbank.com ?

WARREN KUMARI : Non, je ne sais pas. Par contre, ce que je sais, c'est que le www.bigbank.com se trouve au 2.2.2.2. Allez-lui demander.

ORATEUR NON-IDENTIFIÉ : Bonjour www.bigbank.com. Est-ce que vous savez où se trouve le www.bigbank.com ?

RUSS MUNDY : Ah ! En fait, je sais justement où se trouve le www.bigbank.com. C'est au 2.2.2.2.3.

ORATEUR NON-IDENTIFIÉ : Parfait. 2.2.2.2.3, je vais m'en rappeler. Très bien. Voilà, Joe, l'adresse pour le www.bigbank.com.

WES HARDAKER : Très bien, merci. Maintenant, j'arrive à ma page web. Ah ! Mais j'ai un million de dollars en plus dans mon solde. C'est extraordinaire. Alors attendez un instant parce qu'on va continuer le sketch... Voilà comment fonctionne le DNS actuellement, sans le DNSSEC. Alors c'est un petit peu l'équivalent d'Ugwina, résolveur qui donc discute avec Og. Donc voilà, tout se passe bien.

Le problème, c'est lorsque le diable arrive. Où est-il le diable ? Le voilà. Donc on va faire exactement la même chose, mais cette fois-ci, il y aura peut-être un problème, ce monsieur en noir là-bas. Alors moi, je me suis dit, avec mon million de dollars, je peux me payer une maison. Donc je vais sur mon ordinateur, je vais transférer mon argent pour l'emprunt. Donc je vais au www.bigbank.com. Mais mon navigateur ne se souvient plus donc je vais aller voir mon FSI. C'était hier, peut-être qu'il se rappelle des informations.

ORATEUR NON-IDENTIFIÉ : Pardon. Comment vous appelez-vous ?

WES HARDAKER : Joe.

ORATEUR NON-IDENTIFIÉ : Bonjour Joe, enchanté. Vous voulez aller au www.bigbank.com ? Donc je ne sais pas comment faire. Je vais aller voir la racine.

La racine, bonjour. Est-ce que vous savez où se trouve le www.bigbank.com ?

CATHY : On vous voit tous les jours ! Je ne suis pas sûre mais je vais vous envoyer au .com, 1.1.1.1.

ORATEUR NON-IDENTIFIÉ : Très bien, j'y vais. Bonjour monsieur .com. Est-ce que vous savez où se trouve le www.bigbank.com ?

WARREN KUMARI : Non, désolé. Par contre, ce que je sais, c'est que les services de noms sont au 2.2.2.2. Allez leur demander.

ORATEUR NON-IDENTIFIÉ : 2.2.2.2, très bien, je connais je crois. 2.2.2.2, bonjour monsieur www.bigbank.com. Je voudrais me rendre sur le www.bigbank.com. Vous savez où c'est ?

DIABLE : Oui, bien sûr. C'est au 6.6.6.6.

ORATEUR NON-IDENTIFIÉ : Ah, très bien. Merci. Parfait, je vais donner cela à mon utilisateur. Joe, voilà l'adresse de la banque : 6.6.6.6. Bonne chance avec les transactions.

WES HARDAKER : Ah, super. Argent transféré et tout va bien. Alors vous voyez un petit peu comme cela se passe, le problème. Parce qu'en réalité, mon résolveur, mon FSI, ne sait absolument pas qui croire, quel est le signal qu'il peut croire. Il ne sait pas quel est le bon. Donc il prend le premier. Et étant donné que le diable s'est présenté en premier, c'est la première réponse que le résolveur a eue et il y a cru.

C'est un peu l'équivalent d'Ugwina, résolveur qui est perdu et ne sait pas qui est le vrai Og. Donc à un haut niveau, n'importe quel endroit de l'arbre peut être empoisonné. Donc à chaque fois, le résolveur doit s'assurer d'avoir la bonne réponse. Vous voyez qu'en bas, il y a deux Big Bank : une bonne Big Bank et une mauvaise Big Bank. Donc le DNSSEC, c'est en fait la solution à tout ceci qui a été mise au point au cours des quelques dernières décennies, d'abord les spécification, ensuite déploiement, la

racine a été signée. C'est vous l'expert, n'est-ce pas ? Cela fait six ans, je crois, six ans que la racine a été signée. C'était en 2010.

Donc les DNSSEC, ce sont des signatures numériques qui permettent de s'assurer que les informations sont justes. C'est la même chose que la fumée bleue, donc la réponse est claire. Les clés, les signatures vérifient que les informations sont stockées dans le DNS ainsi que dans le cache. Cela ne veut pas dire qu'il y a davantage de transactions qui doivent se passer. Une fois que les informations sont communiquées, tout est caché : la signature et les données. Et étant donné que le DNS est un système de recherches, les clés peuvent être retirées également. Donc le résolveur connaît la clé racine et c'est importante, parce qu'il ne peut pas mémoriser toutes les clés de toute la hiérarchie du DNS. Donc il faut qu'il y ait un point de départ sécurisé.

Ceci commence par une chaîne de confiance. Chaque niveau de la clé signe le niveau suivant, jusqu'à ce que la chaîne soit terminée. Donc les serveurs faisant autorité vous aident au fur et à mesure de la chaîne. Donc voilà comment le résolveur peut cocher à côté de la réponse. Il sait que le casier rouge est mauvais parce que la signature n'était pas la bonne, que vous avez reçu de mauvaises informations. Et donc il va continuer d'essayer d'obtenir des informations jusqu'à arriver à la bonne information. Alors voilà ce qui se passe en matière de DNSSEC.

Donc même sketch et dernière scène avec le DNSSEC. Alors où est ma question ? Merci. Alors je vais donc vérifier ce qui me reste en banque pour voir si mon emprunt a bien fonctionné.

ORATEUR NON-IDENTIFIÉ : Alors je suis le résolveur. Et donc la seule chose que je connais, c'est la clé pour la racine. Je sais que Cathy est mon ancre de confiance. Et donc mon petit autocollant violet, c'est le même que le sien qui est rose. Alors moi, je donne ma signature à Cathy de manière à ce que Cathy sache à quoi ressemble ma signature.

WARREN KUMARI : Voilà, Cathy, à quoi ressemble ma signature : elle est belle, elle est verte, vous voyez.

CATHY : OK, cela marche, très bien.

WARREN KUMARI : Alors moi, il faut que je connaisse la signature de Big Bank. Big Bank, bonjour. Quelle est votre signature ?

RUSS MUNDY : Bonjour .com. Moi, ma signature est une flèche bleue. Comme cela, vous savez à quoi cela ressemble. La voici.

WES HARDAKER : Très bien. Alors maintenant, je vais dans ma banque. Ils ont tout relié et la chaîne est sécurisée. Mon résolveur n'a pas besoin de connaître toute la chaîne. C'est important. Le résolveur n'a eu qu'un autocollant parce qu'il y a beaucoup de résolveurs, beaucoup de FSI dans le monde entier et en fait, ils ne doivent mémoriser qu'une partie des informations.

Alors je vais voir mon FSI et je lui dis : « Oui, j'ai essayé sur mon site de compte en banque. Est-ce que vous pouvez m'aider ? »

ORATEUR NON-IDENTIFIÉ : Cela s'est bien passé en fait la dernière fois ? J'ai oublié de vous demander ? Je ne sais pas où est le www.bigbank.com. Par contre, je vais essayer de m'informer. Alors je vais d'abord me rendre dans la racine. Bonjour racine ! Est-ce que vous savez où est le www.bigbank.com ?

CATHY : C'est vous encore ? Écoutez, je ne sais pas où ça se trouve. Par contre, je sais où est le .com : 1.1.1.1. Mais attendez, je dois vous dire à quoi ressemble la signature. Donc vérifiez d'abord la signature.

ORATEUR NON-IDENTIFIÉ : Oui, effectivement. Je vais vérifier, je vérifie la mienne, regardez la vôtre, OK, très bien, toutes les couleurs sont bonnes ? Très bien. Alors bonjour 1.1.1.1. Je veux me rendre au www.bigbank.com. Est-ce que vous savez où c'est ?

WARREN KUMARI : Je ne sais pas. Mais je sais que le www.bigbank.com est au 2.2.2.2. Voilà ma signature et le www.bigbank.com, sa signature est comme cela ; elle est bleue.

ORATEUR NON-IDENTIFIÉ : Je suis venu chez 2.2.2.2., j'ai vérifié ici, j'ai vérifié chez vous, tout vas bien. OK, très bien. Je vais maintenant au 2.2.2.2. Bonjour Big Bank. Je veux aller au www.bigbank.com.

DIABLE : Oui, je sais. C'est au 6.6.6.6.

ORATEUR NON-IDENTIFIÉ : Alors je vérifie ma signature,... Ah mais attendez, ce n'est pas la bonne adresse ! Cela ne vas pas ! Voilà la sécurité par couches. Bonjour Big Bank, me revoici. Je veux aller au www.bigbank.com. Est-ce que vous savez où c'est ?

RUSS MUNDY : Oui, je sais. Merci d'avoir posé la question. J'ai d'ailleurs un joli petit autocollant bleu que je mets ici. Cela ressemble maintenant à votre étoile.

ORATEUR NON-IDENTIFIÉ : C'est parfait. 2.2.2.3. Toutes les signatures sont valides, tout est parfait, impeccable. Je vais parler à Joe. Bonjour Joe, voici l'adresse et je vous garantie que c'est la bonne.

WES HARDAKER : Oui mais la dernière fois, cela n'a pas bien marché. Vous êtes sûr ?

ORATEUR NON-IDENTIFIÉ : Oui, absolument.

WES HARDAKER : Merci beaucoup. Je suis bien content que vous ayez des mécanismes de sécurité à jour.

Allez, on les applaudit, c'était magnifique. Merci beaucoup. Comme toujours c'était merveilleux.

Alors passons maintenant à la suite. Comme tout à l'heure, Ugwina peut maintenant vérifier les messages, s'assurer que les réponses DNS sont les bonnes. Donc à partir de là, je vais passer

la parole à Russ Mundy, mon collègue, qui va vous expliquer pourquoi vous avez besoin des DSSEC. Donc c'est un guide très simple de déploiement. Il va vous donner d'autres exemples pour vous expliquer comment cela peut vous éviter des attaques.

RUSS MUNDY : Merci Wes. Alors je vais essayer de me mettre dans un endroit où je ne suis pas aveuglé par la lumière et où je peux voir les diapositives. Alors pourquoi a-t-on besoin des DNSSEC ? Qui attaque le DNS ? Personne. En fait, ils attaquent ce que le DNS soutient, tout ce qui est courriels, chat, les services bancaires. Tout ce qui se passe sur internet, c'est cela la cible des attaques, ce n'est pas le DNS en lui-même parce que l'objectif, c'est d'attaquer les applications. Donc aujourd'hui, il y a très peu d'applications qui sont utilisées sur l'internet et qui n'utilisent pas le DNS.

Alors voilà, c'est la bonne diapositive. Alors quels sont les résultats ? Comment est-ce que ces attaques fonctionnent ? Et bien, lorsqu'on commence à, par exemple, ouvrir son compte, sa messagerie courriel, vous le faites sur une machine locale mais parfois, vos courriels sont envoyés quelque part et il arrive que les mots de passe soient volés. C'est la première option. Si par exemple vous rentrez par le réseau à distance, vous pouvez avoir

ce problème de vol de mot de passe. Il y a des applications qui permettent de l'éviter mais quand même, cela est possible.

S'il y a piratage, par exemple enregistrement de communications, vous observez ce qui se passe et encore une fois, il existe des mécanismes qui sont associés avec ceci et qui permettent d'éviter ce type de problème. Et si quelqu'un veut davantage de détails par rapport ces applications, sachez que mercredi, il y aura un atelier sur les DNSSEC avec quelques présentations qui vous permettrons de connaître davantage d'informations sur l'amélioration de la sécurité du DNS, des courriels et autres grâce à la technologie qui existe.

Alors ce qui est important de se souvenir en termes simples par rapport au DNS, c'est qu'on peut facilement le contourner. On faisait un cours sur le piratage du DNS auparavant mais c'est devenu un petit peu ennuyeux lorsqu'on faisait ces présentations pendant ces années. Maintenant, il est illégal de faire du piratage de DNS. Donc de toute façon, ce n'est plus d'actualité.

Donc en termes d'outils qui existent actuellement, il existe plusieurs outils disponibles contre le piratage du DNS, qui sont disponibles sur l'internet. Et ensuite, vous pouvez pirater des sessions qui soutiennent le DNS.

Donc vous avez vu notre petite mise en scène. Ensuite, la BD avec Ugwina. Et le DNSSEC, c'est comme la fumée bleue. Donc lorsque l'utilisateur Joe obtient finalement la réponse de la part de son FSI et que cela a été signé, cette signature garantie le fait qu'effectivement, les informations qui lui sont revenues, c'est ce qu'on appelle l'intégrité des données et l'authentification de la source et tout le jargon technique, informatique, on peut être sûr d'où proviennent ces informations qui sont authentifiées.

Donc là, vous avez un petit exemple avec des images qui vous montre l'utilisateur Joe qui envoie une requête. Mon dieu, normalement, je file très vite là-dessus mais là bon, je vais aller un petit peu moins vite. Donc la requête de l'utilisateur Joe est envoyée vers son FSI, fournisseur de service internet, puis vers le serveur. Il pose la question, la réponse revient et une fois que la réponse revient au FSI, alors cet utilisateur Joe peut faire ce que bon lui semble, c'est-à-dire transaction bancaire. Cela est un petit exemple sous forme très imagée de ce qui se produit. Et c'est beaucoup plus simple de le comprendre de cette manière.

Donc lorsque vous procédez à ce genre de vérification, parfois, vous voyez que vous avez passé avec succès la vérification DNSSEC. Là, c'est un navigateur qui a été modifié pour vous montrer ce qu'on voit lorsqu'il y a vérification positive du DNSSEC. Et ici, c'est un navigateur qui n'a pas reçu cette vérification du DNSSEC.

Si vous regardez de près, ce que vous voyez, c'est qu'il y a un texte sur ces deux écrans. Et c'est le même texte. Pourquoi est-ce que je n'arrive pas à avancer dans cette présentation ? Oui, voilà, je vois que le diable s'en est mêlé. Voilà, je l'ai.

Donc la question est de nouveau posée. Elle est envoyée au résolveur récursif. Mais attention, le pirate, le méchant est là. Il guette, il voit qu'il y a une requête envoyée et il veut répondre d'abord. Et c'est ce qu'il fait, d'ailleurs. Mais lorsqu'il le fait, plutôt que d'envoyer vers le bon site web, il l'envoie vers un mauvais site web, celui du méchant.

Donc entre temps, les autres requêtes seront envoyées, répondues. Mais la requête de l'utilisateur Joe, elle, est renvoyée vers un site web, le site web du méchant. Et lorsque la vérification DNSSEC échoue, plutôt que d'aller vers le site web du méchant, l'utilisateur Joe va effectivement aller vers le bon site web. Donc il reçoit une réponse en retour et nous y voici.

Dans ce cas-là, ce qu'on a fait, vous voyez ici des print écran de certains exemples de piratage qu'on a fait il y a quelques années et du coup concernant le piratage du DNS. Vous voyez ici, le navigateur en bas ne fait pas de vérification DNSSEC et vous voyez, le contenu sur la page n'est plus le même. Et de fait, ce qui a été fait dans cet exemple pour voir comment utiliser un piratage DNS, c'est qu'on a inséré des informations. Il s'agit du

même site web, à une différence près, à savoir que cet URL et ce nom DNS ont été piratés et l'utilisateur pense qu'il est en train de voir la bonne information et ce n'est pas le cas ; il voit d'autres informations. Et cela a été fait à l'époque où Steve Crocker était président du Conseil d'Administration de l'ICANN, tout le monde le connaît. Et il n'a jamais dit que le monde allait être sauvé de la faim.

Vous voyez ici une page avec le nombre de requêtes envoyées pour une page. Et cela, c'est la même page, cinq ans plus tard. Comme vous voyez, il y a des requêtes DNS de plus en plus nombreuses et complexes pour une seule même page montrée par un navigateur.

Donc ce qui est important de se souvenir par rapport à ce que fait le DNS, c'est que le DNS protège les informations elles-mêmes contenues dans le DNS. Et sans trop rentrer dans le détail de la manière dont cela est effectué, ce qui est important de retenir, c'est que les informations dans la zone du DNS sont toutes aussi importantes que tout autre matériel cryptographique contenu dans la zone du DNS utilisé pour accomplir les fonctions du DNSSEC. Donc finalement, la grande question importante à retenir, c'est que le DNSSEC permet de vérifier et valider le navigateur de l'utilisateur.

Autre image pour vous montrer le va-et-vient des informations. Cela, c'est sans DNSSEC.

Donc quelques mots par rapport à la mise en œuvre Alors je reviens à cette diapositive. Si vous êtes assis ici où se trouve l'utilisateur Joe avec le client et vous, vous n'opérez pas le DNS pour vous-même mais quelqu'un le fait à votre place. Donc vous avez besoin de déterminer de quelle manière les services du DNS sont fournis. Et vous examinez cela et certaines organisations qui viennent aux réunions ICANN sont très centrées sur les questions liées au DNS, ont beaucoup de connaissances et d'expérience en matière de DNS et opèrent le DNS elles-mêmes. D'autres n'ont pas autant de connaissances et ne le font pas elles-mêmes.

Donc si vous êtes une entreprise qui s'y connaît très bien en termes de DNS, vous allez probablement opérer vous-même vos opérations DNSSEC. Si au contraire vos activités qui impliquent le DNS sont importantes mais vous n'êtes pas vous-même expert en DNS et que vous faites appel à une autre organisation pour opérer le DNS, alors il convient de se poser la question est-ce qu'il faut que moi-même j'opère le DNSSEC ou je fasse appelle à une autre entreprise pour qu'elle s'en occupe. Mais comme vous le voyez ici, la question qui se pose et qui est importante, c'est de protéger les données de la zone DNS. Et quoi que vous fassiez dans les opérations DNS, il faut toujours faire un parallèle par

rapport aux opérations du DNSSEC, comme si c'était une capacité supplémentaire que vous ajoutez dans le DNS. Et vous pouvez vous inspirer de la manière font vous opérez les opérations du DNS actuellement.

Donc par rapport aux informations du DNSSEC, comme on l'a fait pendant la petite mise en scène, vous échangez vos clés et le résolveur récursif vérifie que ces signatures sont bonnes. Et là, c'est une illustration très simple pour reprendre la même idée, là, cela montre bien que la zone et signée et ici, c'est là que la validation a lieu. Et donc ce sont des mesures, des étapes, des fonctions supplémentaires que vous ajoutez dans vos opérations liées au DNS actuel.

Donc cela, c'est le principe général. Quelle que soit la manière dont vous opérez votre DNS, que vous le fassiez vous-même ou d'autres le font, il faut penser à la validation du DNSSEC dans vos opérations actuelles. Si vous faites appel à nous, une autre organisation, et que votre organisation ne le fait pas actuellement, alors il faut que vous travailliez avec votre sous-traitant pour vous assurer que ce sous-traitant peut vous fournir la vérification DNSSEC. Et si ce n'est pas le cas, je vous encouragerais à chercher un fournisseur DNS qui lui pourra vous donner les capacités et fonctions DNSSEC.

Cela, c'est pour ce qui concerne notre présentation. Et comme je l'ai dit auparavant, nous avons un certain nombre de personnes dans la salle qui connaissent le DNSSEC sous tous ses aspects. Donc je vous encourage à poser des questions mais je vais céder la parole à Wes.

WES HARDAKER : Merci. Alors j'aimerais conclure avec quelques informations supplémentaires et on n'a pas de diapositives là-dessus, d'ailleurs. Vous aurez remarqué que le DNSSEC continue à être actualisé. D'ailleurs, sachez qu'il y a des chaises ici à l'avant. Si vous avez besoin de vous asseoir, ne vous gênez pas.

Donc il y a beaucoup de choses qui sont en train de se produire actuellement. Vous aurez entendu que l'ICANN est en plein roulement de la clé actuellement. Vous vous souvenez de la fumée bleue au fond de la grotte ? On recommande un changement vers une nouvelle clé régulièrement et il y a un processus pour ce faire de manière sécurisée puisque vous l'avez vu dans le petit sketch, la fumée change de couleur. Donc si vous envisagez de passer du bleu au vert, on peut se rendre compte clairement que cela n'est pas le bon signal qui est émis. Mais voilà où on en est un petit peu actuellement.

L'ICANN, par l'intermédiaire de l'IANA, est en train de transmettre des signaux de fumée bleue et vert à la fois. Donc à

un moment donné, on va supprimer ce signal de fumée bleue. Mais cela implique toute une série de difficultés techniques parce qu'il faut s'assurer que tout le monde obtient la même clé.

Alors est-ce qu'il y a des questions dans la salle par rapport à ce qu'on vous a dit aujourd'hui, le DNSSEC, le déploiement ? Ce que vous voulez. Posez vos questions et on va bien trouver une personne qui va y répondre.

LENDON TELESFORD : Bonjour, Lendon de Grenade. J'ai une question par rapport à votre petit sketch et vos diapositives. En fait, je ne suis pas sûr parce que je suis boursier pour la première fois, je ne suis pas sûr que ma question soit pertinente, mais bon. Alors en fonction de l'exemple que vous avez donné, j'ai l'impression que c'est une chaîne de confiance. N'est-ce pas ? Vous avez parlé de chaîne de confiance. Et peut-être que c'était un peu sous jacent mais moi, je ne vois pas cette relation entre le client et le fournisseur par rapport au résolveur du DNSSEC.

WES HARDAKER : Alors est-ce qu'on a une petite récompense parce que ça, c'est une question brillante. Est-ce que quelqu'un veut y répondre ? Viktor ?

VIKTOR DUKHOVNI : Oui. Alors pour les questions qui ont à voir avec la sécurité DNSSEC, cela a à voir avec l'homme du milieu entre le résolveur et le fournisseur. Vous pouvez envoyer une requête mais si vous posez la question au résolveur du FSI, alors peut-être que là, il peut se poser un problème. Ce qui est important, c'est d'être sûr que le FSI ne sera pas compromis par des données stockées depuis longtemps. Et ensuite, cinq minutes après, si vous demandez la même requête, vous vous rendrez compte si vous obtenez la même réponse ou pas.

WES HARDAKER : Oui, effectivement. Et information supplémentaire, le problème que vous venez de décrire, c'est justement le problème ultime qu'on appelle *last mile* en anglais. Donc on peut le faire sur le résolveur lui-même et Viktor, c'est justement celui qui travaille sur la sécurité des courriels au DNSSEC, un expert extraordinaire dans la salle.

Autre information. L'IETF – c'est l'organe qui a créé les protocoles internet, la manière dont fonctionnent les courriels, etc. – est actuellement en train d'examiner la question de la vie privée et confidentialité des courriels par rapport aux attaques de l'homme du milieu, la relation entre chaque client et le résolveur.

Donc à l'avenir, ce mécanisme de protection va également pouvoir vous protéger des attaques de l'homme du milieu. Donc il s'agira d'une chaîne sécurisée. Ce sera une chaîne différente de celle du DNSSEC mais elle continuera de vous protéger.

Russ ?

RUSS MUNDY : J'aimerais ajouter quelque chose. Beaucoup de gens sont sceptiques lorsqu'ils voient tout ce processus cryptographique. Ce n'est pas un problème par rapport au DNNSEC. Cela a été réglé dès la conception du DNNSEC. Avant, j'avais un téléphone portable qui faisait cette vérification DNNSEC sur le portable lui-même. Donc même sur ces petits dispositifs, vous pouvez faire une vérification DNNSEC. C'est ce sur quoi on peut éventuellement tendre pour l'avenir.

WES HARDAKER : Autres questions dans la salle ? Allez-y, allez-y.

GERARD BEST : Gerard Best de Trinité-et-Tobago. Alors je vais essayer d'être à la hauteur de la question précédente. Alors ma question porte sur les résolveurs 8.8.8.8. et 9.9.9.9., et j'aimerais savoir si ces résolveurs ouverts... enfin connaître vos point de vue d'experts

par rapport à la vigueur de ces mécanismes de la sécurité de l'internet.

WES HARDAKER : Excellente question à nouveau. C'est la même question de la relation entre vous-même et le résolveur. Sachez que j'ai une personne ici qui peut parfaitement répondre à votre question. N'est-ce pas, Warren ? Est-ce que vous pouvez faire un commentaire ? Est-ce que vous voulez deviner pour qui travaille Warren ?

WARREN KUMARI : Oui, je travaille pour Google. Alors il y a une vérification DNSSEC tous les jours qui est faite avec Comcast et avec des grands résolveurs qui ont commencé à utiliser DNSSEC. Donc effectivement, il y a énormément de gens qui suivent de près cela de manière très sérieuse. Moi aussi je le faisais mais cela dépend de votre propre décision.

WES HARDAKER : Est-ce qu'il y a quelqu'un ici qui travailler pour PCH ?

ORATEUR NON-IDENTIFIÉ : Oui. Nous aussi, nous faisons de la validation DNSSEC et il y a un autre outil qu'on peut utiliser en cas de suspicion d'échec de validation DNSSEC.

WES HARDAKER : Bien. Eux, ce qu'il font aussi, c'est du TLS, c'est ce dont on parlait auparavant : protéger les mécanismes et être sûr que vous obtenez la bonne réponse de la part du résolveur. Donc excellente question. Merci.

Y a-t-il d'autres questions ? Il y en avait une là-bas.

RAPHAEL VICENTE ROSA : Je suis NextGen. Nous avons vu un diagramme pour savoir comment une simple requête auprès de cnn.com est résolue. C'était un gros diagramme. Donc ce que je voudrais savoir, c'est l'impact sur la performance si on a le DNSSEC en plus ou alors est-ce que vous le montrez déjà ?

WES HARDAKER : Cela a été conjointement avec Russ et moi. Donc cela, c'est mon ordinateur, là et à côté, le sien. C'est quelque chose que l'on a fait il y a un certain temps et oui, vous avez le DNSSEC. Si vous regardez en orange, en fait les lignes ne sont pas sécurisées. Donc en grande partie, ce n'est pas sécurisé. Mais si vous

regardez bien, vous avez du vert aussi. Donc ça, c'était au tout début. On s'est dit qu'il fallait qu'on fasse une autre série. On devrait peut-être le faire cette semaine parce que le diagramme aurait meilleur aspect. Il y a encore beaucoup de déploiement qui n'a pas été fait et qui reste à faire. Mais en termes de performance, est-ce que vous voulez faire un commentaire là-dessus ? Je ne sais pas, vous avez mentionné quelque chose tout à l'heure. Est-ce que vous avez fait des analyses par rapport au DNSSEC et par rapport aux connexions TLS sur le web ?

ORATEUR NON-IDENTIFIÉ : Dans la plupart des cas, les informations sont cachées, sont dans le cache, donc ce sont des réponses plus larges. Mais il n'y a pas davantage de requêtes, surtout si votre consommateur fait une requête au FSI, il reçoit la même réponse. Mais cela n'a pas beaucoup d'impacts sur vous. En fait, quand les utilisateurs font la même requête, c'est comme cela que cela se passe.

WES HARDAKER : Cela répond à votre question ?

WARREN KUMARI : Oui. Il y a également un suivi par rapport à cela. Dans certains cas limités, les choses vont plus vite grâce au DNSSEC parce qu'on reçoit une réponse, une preuve qui vous dit que la

réponse est la bonne. Dans ces cas, les réponses négatives, lorsque par exemple vous faites une erreur de frappe, cela est résolu instantanément. Et également toutes les réponses qui viennent de wildcards, qui est un enregistrement qui dit que tout est mappé là-dessus, donc cela aussi vient de votre résolveur sans avoir à demander aux autres serveurs faisant autorité. Donc c'est un processus d'accélération limité. Et en cas d'attaque, voilà comment cela fonctionne.

WES HARDAKER : D'autres questions ? Ici oui, à l'avant.

ORATEUR NON-IDENTIFIÉ s: S'il y a un échange de clés entre les différents serveurs, donc cela se passe lorsqu'une requête a lieu. Donc l'utilisateur, en fait la personne qui s'occupe de l'échange des clés doit savoir quelle est la communication ? Comment cela marche ? Comment la clé est cachée ?

WES HARDAKER : Excellente question, je vais y répondre. Vous vous souvenez qu'au début, j'avais dit que les clés, on peut les rechercher dans le DNS comme le reste. Donc on pourrait passer par toute une chaîne assez complexe pour savoir un petit peu en quoi la clé est incluse dans tout le processus. On ne vous a pas tout montré

parce qu'il y a beaucoup plus de requêtes, donc ce serait beaucoup plus long. Mais par exemple, sur www.example.com, le FSI va demander non seulement où se trouve www.example.com mais va demander quelle est la clé pour www.example.com. Il va vérifier la signature de la clé également. Donc vous avez vu que les gens ont vérifié les clés mais il y a encore d'autres requêtes qui entrent en compte. Et ceci est fait en parallèle suivant le code du résolveur. Cela dépend. Donc il y a d'autres processus qui sont impliqués. Et donc il y a des vérifications de signature à chaque niveau de l'arbre. Est-ce que cela répond à votre question ?

ORATEUR NON-IDENTIFIÉ : Oui.

WES HARDAKER : Y a-t-il d'autres question ? J'en vois pas mal, d'ailleurs.

ORATEUR NON-IDENTIFIÉ : Donc la sécurité dans ce processus dépendait du petit autocollant que vous avez distribué au début du sketch. N'est-ce pas ? Et cela, en fait, je n'ai pas bien compris. Comment est-ce que vous allez organiser cette distribution des autocollants et également, à quelle fréquence vous devez le faire ? Je pense que cela fait partie de la question de tout à l'heure.

WES HARDAKER : Excellente question, effectivement.

VIKTOR DUKHOVNI : Alors justement, je voulais parler de ceci parce que c'est une question qui est importante. Ce qui n'a pas été mentionnée pendant le sketch, c'est que la sécurité se passe non seulement entre l'utilisateur et la banque mais également entre l'autorité de certification et la banque parce que dans la vie réelle, la sécurité dépend du certificat qui est obtenu par la banque, à savoir si le certificat est juste ou pas. Et donc lorsque les autorités donnent le certificat à la banque, c'est là que la sécurité a lieu. Et en fait au début, on ne sait pas en fait. C'est toute une illusion. Les autorités donnent à leurs clients des certificats sans savoir vraiment qui ils sont. C'est la question de la validation des domaines. Et pour la plupart d'entre vous, vous seriez choqués si je vous disais à quel point cela manque de sécurité.

Alors les DNSSEC permettent de sécuriser cela. Il y a un petit peu plus d'ajout du DNSSEC pour que les domaines qui sont signés avec le DNSSEC soient plus protégés lors de l'émission de ces certificats. Et donc cela veut dire que l'utilisateur est mieux protégé.

La raison pour laquelle je parle des CA, c'est parce que tout ce que font ces CA, c'est que cette partie du domaine est contrôlée par telle personne. Mais en fait les personnes qui savent qui contrôle le domaine, c'est les bureaux d'enregistrement. Lorsque vous achetez un domaine auprès du bureau d'enregistrement, il vous appartient. Donc les autocollants que vous obtenez sont publiés par les bureaux d'enregistrement dans le DNS. Et c'est vous qui alimentez les données au bureau d'enregistrement. Vous signez le domaine, vous dites à votre bureau d'enregistrement que vous avez besoin d'un autocollant. Et donc il est acheté. Il n'y a pas de partie tierce. L'autorité de certification de dit pas : « Et au fait, Big Bank, c'est telle personne. Donc... » En fait, ce qui se passe, c'est le bureau d'enregistrement avec lequel vous avez une relation directe, sans partie tierce qui connaisse tout, qui publie les clés. Alors il faut le faire de temps à autre, au fur et à mesure du changement des clés. Si vous ne changez pas vos clés, vous n'allez pas avoir d'autocollant. Si vous les roulez régulièrement, vous devez coordonner le roulement de clés avec le bureau d'enregistrement.

Donc c'est une longue réponse. Il y a beaucoup plus de choses qui sont impliquées. Je ne vais pas tout vous dire mais j'espère que cela est clair.

WES HARDAKER : C'est l'équivalent, donc, l'exemple, pour faire le suivi, c'est tout à fait cela en fait. Si vous allez enregistrer un nouveau domaine avec un bureau d'enregistrement, par exemple vous utilisez GoDaddy ou peu importe, lorsque vous allez les voir, ceux qui soutiennent le DNSSEC ont un petit casier dans lequel vous mettez votre clé. Donc vous pouvez le modifier après, lorsque vous signez. Et c'est ce qui ajoute cette transition de l'autocollant. Donc le détenteur du domaine le fait pendant le processus d'enregistrement du domaine. C'est bon ? C'est clair ? Russ ?

RUSS MUNDY : Je voulais mentionner encore un autre point. Dans ma présentation, j'ai mentionné que votre organisation et son implication dans les opérations, que ce soit dans le cadre d'un ccTLD ou d'un GTLD, veut dire que si vous gérez votre DNS, et bien il sera peut-être bon de gérer les mécanismes DNSSEC qui y sont associés avec la coopération du bureau d'enregistrement pour avoir la clé directement dans le système DNS. Si votre DNS est géré par, par exemple, votre opérateur de registre, ce qui est très courant, c'est le bureau d'enregistrement lui-même qui peut s'occuper de tout cela pour vous. Il y a des recommandations par rapport à la fréquence du roulement des clés mais tout ceci peut être automatisé. Et dans la plus part des cas, le point de vue général est qu'il est mieux que tout ceci soit automatisé

parce que comme cela, il n'y a pas des gens qui, avec des doigts sur les claviers, font des erreurs ou qui oublient de faire certains changement. C'est 30 jours, six mois, un an, cela dépend en fait de la fréquence de changement.

WES HARDAKER : Beaucoup de bureaux d'enregistrement ont des cases à cocher. Si par exemple vous utilisez leurs services, vous pouvez cocher la case DNSSEC. Parfois, c'est même par défaut. Il est tout à fait possible que vous ayez accès à ce service et que vous ne le saviez pas.

Autres questions ?

MUJIBULLAH SHAMS : Bonjour. Je suis boursier ICANN. Les DNSSEC signent les requêtes et les réponses. Maintenant, quel est le mécanisme de cryptographie utilisé par les DNSSEC utilisé pour signer ces requêtes et ces réponses ? Deuxième question : lorsque le roulement se passe, quel est le mécanisme utilisé pour partager la clé entre les parties qui font partie de l'échange ?

WES HARDAKER : Du point de vue cryptographique, c'est un mécanisme de clé privé qui s'occupe de la signature, tout à fait similaire au PGP ou

au certificat web. Donc le détenteur de la clé a une copie privée à laquelle personne n'a accès. Et donc il y a une autre clé publique qui est utilisée pour la validation. La longueur de la clé varie. Cela dépend du détenteur de zone, donc 512 à plus de 4096 bytes. Donc tous ces types de choses existent.

En ce qui concerne le roulement, il y a un RFC qui définit le mécanisme de roulement. Nous parlons de roulement de KSK, avec la racine. Donc lorsque vous avez une zone, lorsque vous avez besoin de changer votre clé, vous devez aller vous adresser à votre bureau d'enregistrement. Le .com publiera des références à vos deux clés pendant l'instant. Donc vous attendez un petit instant et en fin de compte, vous changez. Donc il y a une période où le reste du monde s'apercevra sans doute que vous avez deux clés publiées et que les deux sont valides. Et ensuite, vous éliminerez les anciennes versions. Donc effectivement, il y a tout un timing à prendre en compte.

WARREN KUMARI : Comme suivi par rapport à cela, l'ancienne clé, c'est la nouvelle clé actuellement. C'est ce qui se passe pour l'instant. C'est secret mais pas vraiment.

WES HARDAKER : Oui. Question suivante ?

TARAU BAUIA : Nous dépendons du 8.8.8.8. Donc ma question, c'est de savoir si on peut ne pas passer par le FSI. Est-ce qu'on peut utiliser le Google DNS ? Est-ce qu'on peut dupliquer le DNS dans notre propre réseau ?

WES HARDAKER : Vous pouvez avoir un résolveur de validation de DNS dans votre réseau. Vous avez le choix : vous pouvez soit utiliser Google PCH, Comcast, etc., les DNS ouverts. Je crois qu'ils s'occupent de résolution de DNS. Donc il y en a un certain nombre qui sont ouverts que vous pouvez utiliser, ou alors vous pouvez utiliser le vôtre, comme vous le voulez. Et les grands qui sont ouverts s'occupent des DNSSEC. D'ailleurs, ce sont eux qui font la plupart des validations. Il y a un certain nombre de choses qui se passent, je ne sais plus quel est le pourcentage mais il y a quatre à cinq résolveurs.

Autres questions ?

ABDULKARIM OLOYEDE : Bonjour, Abdulkarim. J'aimerais savoir, ces certificats web que vous recevez lorsque vous êtes sur un site web, on vous dit parfois « Ce site web n'est pas sécurisé ». Quel est le lien entre ce message et le DNSSEC ?

WES HARDAKER : Excellente question. Est-ce que quelqu'un d'autre peut répondre ? Pour répondre rapidement, ce n'est pas lié en fait. Lorsque vous recevez la page qui dit « Vous vous rendez sur un site pour lequel le certificat, nous ne lui faisons pas confiance. » Vous vérifiez le certificat alors. Vous avez l'adresse, vous êtes passé par le DNS, votre navigateur a essayé de s'y rendre mais il n'a pas eu confiance ; c'est différent. Donc DNSSEC se passe avant. Vous devez faire une recherche pour www.bigbank.com et ce qu'on n'a pas montré dans le sketch, c'est que si le FSI n'avait pas de réponse valide, en fait, ils revenaient vers moi, Joe user, et ils m'auraient dit : « Désolé » Et à ce moment-là, vous avez site non trouvé, donc hébergement non trouvé. Il y a d'autres exemples plus compliqués de ce qui se passe si le navigateur comprend le DNSSEC, etc. mais voilà.

ABDULKARIM OLOYEDE : Donc la certification, il y a deux certifications en fait. Premièrement...

WES HARDAKER : Oui, effectivement. Il est mieux d'avoir les deux mais c'est en fait deux chemins complètement différents.

VIKTOR DUKHOVNI : Cela se chevauche parce que l'autorité qui émet le certificat, très souvent, utilise des moyens non sécurisés de vérifier que le site est sécurisé, peut-être un DNS non signé. Le CA dit pour vérifier, on sait que c'est vous. Mais il peut y avoir l'homme du milieu. Donc si votre trafic est redirigé vers un autre pays et qu'il y a piratage, s'il y a quelque chose qui se passe, l'attaquant obtient parfois des certificats pour différents sites. Donc le chevauchement, c'est que la validation du CA, détenteur de domaine, n'est pas sécurisée. C'est rare qu'il y ait des attaques. Donc d'une manière générale, les attaques sont rares mais elles sont possibles, quand même.

WES HARDAKER : Et si on avait le DNSSEC partout, cela résoudrait ce problème et cela inclut la validation quand je dis déploiement total.

Autres questions à la table ?

LAUREN BURKHART : Je suis Lauren Burkhart, je suis des États-Unis. J'ai une question de base parce que je ne connais absolument rien par rapport à la technologie. Vous avez parlé du fait que vous pouvez tout simplement cocher les cases, que le DNSSEC peut être géré par le bureau d'enregistrement. Lorsque le déploiement sera total ? Où en est-on en fait ? Est-ce que cette case est souvent cochée ?

WES HARDAKER : Excellente question. Justement, les gens qui s'en occupent sont là avec nous dans la salle. Alors avant de passer la parole à Viktor, je vais mentionner une chose.

Il y a un programme qui s'appelle SECSpider qui est une base de données qui permet d'identifier tous les domaines qui ont été signés. Et le pourcentage n'est pas aussi élevé qu'on pourrait le penser. Le .com par exemple, c'est 0,5 %. Si vous allez à l'atelier DNSSEC, vous verrez, ils en parleront. Mais 0,5 % du .com, c'est plus de 500 000 sites, donc c'est quand même assez élevé.

Il y a des raisons techniques pour lesquelles certaines sociétés n'ont pas encore déployé ceci, parce qu'il y a des questions d'équilibre, etc.

VIKTOR DUKHOVNI : J'ai 5,2 millions de sites qui ont été signés que je suis. Pour la plupart, c'est en Europe du Nord : en Hollande, en Suède, en Allemagne, en Norvège, en République tchèque. Le reste du monde, on n'en est pas là encore. Donc c'est très inégal en fait, le DNSSEC.

Le .com a plus de 800 000 domaines de signés. En Suède, la moitié des domaines, même plus ; en Hollande, la moitié des domaines sont signés. Pour le .bank, il y en a plus. En fait, les

banques enregistrent les marques de commerce mais elles ne les signent pas. Même chose pour l'assurance : tous, ils sont signés mais ils ne sont pas nécessairement utilisés.

Mais d'une manière générale, le chiffre est entre deux-tiers et 1 %. Mais dans certains endroits, l'utilisation est très élevée. Par exemple en Hollande, les DNSSEC sont moins chers. En fait, on vous donne une réduction si vous faites signer avec le DNSSEC pour votre nom de domaine.

En ce qui concerne les TLD, 86 % des TLD sont signés. Mais pour avoir les nouveaux TLD qui sont compatibles avec le DNSSEC, plus de 50 % des pays, tout ce qui est .org, .net., .edu, .biz, .info, tout cela, c'est signé. Donc il y a quand même un grand nombre de premier niveau qui est signé. Nous essayons de convaincre d'autres sociétés maintenant.

LAUREN BURKHART : Est-ce qu'il y a une manière très simple d'expliquer pourquoi est-ce que les gens ne signent pas ? Est- ce qu'il y a des raisons ou est-ce que c'est simplement du travail ?

WES HARDAKER : Russ ?

RUSS MUNDY : C'est les deux. Comme Wes l'a dit tout à l'heure, il y a des organisations qui ont exploité diverses choses que l'on peut faire avec le DNS. Et cela les aide du point de vue commercial, en fait. Ce que ces sociétés font ne fonctionnera pas si elles suivent les règles. Cela permet d'identifier qu'il y a des choses qui ne marchent pas bien. Donc il y a des cas comme cela.

Je crois également qu'un des plus gros problèmes, c'est un problème de formation des gens. Et c'est pour cela, justement, que nous organisons ce type de session, pour que les gens soient familiarisés avec les bases en matière de sécurité du DNS. Il faut qu'il y ait davantage de personnes dans le monde qui comprennent la situation et qui reviennent vers leurs organisations dans le cadre de leur travail et qu'ils commencent à poser des questions : « Pourquoi est-ce que nous n'avons pas sécurisé notre système ? Que puis-je faire pour faire avancer les choses ? » C'est très important. C'est vraiment une partie intégrante de notre séance.

JACQUES LATOUR : Je travail avec .ca. Nous avons 2,7 millions de noms de domaine au Canada actuellement et 1 000 ont été signés avec le DNSSEC, donc c'est un pourcentage très faible, 0,0... quelque chose. Donc le défi consiste à travailler là-dessus, justement. Les bureaux d'enregistrement qu'on a, pour certains, ils soutiennent le

DNSSEC. Et les titulaires de nom de domaine doivent payer plus pour le permettre. Donc c'est un défi. Il faut payer plus pour obtenir de la sécurité. Et souvent, c'est un jeu pour les titulaires de nom de domaine. Le coût, c'est un problème pour le déploiement du DNSSEC.

WES HARDAKER : Andrew, oui ? Il y a une question dans la salle.

ABDALMONEM GALILA : Abdalmonem de l'Égypte. Alors je ne fais confiance à personne. Donc je vais faire mon validateur DNSSEC sur ma machine. Je pense qu'il faut s'éloigner de l'attaque de l'homme du milieu entre mon FSI et moi-même. Donc pourquoi ne pas conseiller à tous d'avoir un validateur local sur son ordinateur ?

WES HARDAKER : Excellente question. Viktor ?

VIKTOR DUKHOVNI : Si vous avez un dispositif mobile, malheureusement, il y a beaucoup d'environnements qui sont hostiles au DNSSEC parce que l'infrastructure qu'ils ont, les portails qu'ils utilisent, il faut accepter leurs termes et conditions, etc. Quel que soit le site que vous tapez, Google.com, il y a un portail qui s'ouvre. Donc pour

une raison ou pour une autre, il faut mettre en place les politiques qui modifient les réponses DNS. Donc la plupart des dispositifs mobiles actuellement ne peuvent pas supporter une validation DNSSEC sur ces dispositifs.

WES HARDAKER : Russ ?

RUSS MUNDY : Oui, c'est une très bonne chose que vous venez de soulever, Viktor. On peut prendre en considération ce genre de problème. Il y a un logiciel qui s'appelle DNSSEC-Trigger de NLnetLabs qui a été spécifiquement conçu pour ce genre de cas de figure. Et il a un certain nombre de mécanismes qui lui sont inhérents. Et il est très difficile de faire du DNSSEC.

Et si je me souviens bien, dans le genre de situation et environnement que décrit Viktor, la première connexion doit être faite sur l'hôtel parce que sinon, l'accès est bloqué. Mais ensuite, on commence à faire du DNSSEC parce que vous pouvez ensuite y avoir accès. Personnellement, moi, je procède d'une autre manière. Une fois que j'obtiens le blocage de l'hôtel, moi, j'allume mon VPN et je vais sur les serveurs DNS que je connais. Donc il y a plusieurs mécanismes qui vous permettent de

contourner cette difficulté mais ce n'est pas toujours si simple à faire.

WES HARDAKER : Oui mais les choses s'améliorent. Le fait que le DHCP, par exemple, vous demande une connexion et il y a un pop-up qui arrive, une fenêtre, un pop-up qui s'ouvre et vous dit « Il faut vous connecter, etc. » Donc vous pouvez avoir le DNSSEC mis en place localement. Et je vous encourage à le faire si vous êtes expert et vous pouvez le faire. C'est ce vers quoi on tend. Certains fournisseurs, effectivement, le configurent sur leur machine, c'est en train d'apparaître de plus en plus

Est-ce qu'il y a une autre question, Andrew, dans la salle ? Au fond ?

FRANSLEIDY DE JESUS DIAZ : Bonjour, je suis NexGen, Fransleidy Diaz. Est-ce que cela pose un problème si je pose ma question en espagnol ? Est-ce que quelqu'un a des écouteurs ?

WES HARDAKER : Oui, allez-y.

FRANSLEIDY DE JESUS DIAZ : L'un des problèmes du DNS par rapport à la clé, c'est le KSK. Donc le problème, c'est que lorsqu'on obtient l'information et vous ne savez pas si cette information a été modifiée ou pas, c'est pourquoi on a changé la zone racine à KSK. Cela, c'est ce que j'ai cru comprendre de ce qui s'est passé en février. Donc lorsque vous allez opérer les changements, qu'est-ce que vous allez faire pour que ce problème ne survienne pas ?

WES HARDAKER : Attendez pour que la traduction arrive. Et Jacques va répondre à votre question.

JACQUES LATOUR : Je crois que la question, c'est qu'on est en train de rouler la clé parce que la clé actuelle pourrait être comprise ? C'est cela, la question ? Non, ce n'est pas ce qui s'est passé. C'est cela votre question ?

FRANSLEIDY DE JESUS DIAZ : Oui, en février lorsque vous avez, à Los Angeles, fait le KSK, vous avez fait le roulement de clés. Et ce que j'ai vu dans votre présentation, un problème, c'est que la formation était erronée ou qu'il y avait d'autres informations parce que vous avez changé la zone racine.

JACQUES LATOUR : Il y a eu un évènement en février et peut-être que c'était lié à cela, au KSK. Et la deuxième question, qu'est-ce qu'on peut faire par rapport au KSK et donc qu'est-ce que vous faites. C'est trois questions différentes finalement.

RUSS MUNDY : Alors il y a un processus très documenté qui décrit bien la manière dont les KSK sont générés, les premiers, comment sont générés les nouveaux. Et dans cette première partie du processus, il y a des gens totalement indépendants qui ont été identifiés au préalable comme des personnes qui soutiennent la communauté et qui peuvent être témoins du fait que les choses sont faites en bon et due forme. Et le stockage de la clé, une fois qu'elle est générée puisqu'elle est générée sur un dispositif de disque dure, et ce dispositif de disque dur est enfermé lorsqu'il n'est pas utilisé. Et c'est de cette manière que le KSK actuel a été généré et le nouveau KSK a été généré Donc la partie publique du KSK est visible et disponible à tous. Et tout le monde peut le voir et l'utiliser. La partie privée, elle, est très sécurisée, protégée. Et toutes les cérémonies de KSK sont disponibles, tout cela est disponible sur le site web de l'ICANN.

Il y a une norme ISO 9000 qui a été élaborée pour créer toutes ces installations. On a eu deux ou trois audits de la part de

consultants externes pour s'assurer que la clé privée est protégée et sauvegardée très précieusement. Et cela n'a rien à voir avec l'engagement du changement, changement parce que la procédure de changement a stipulé qu'il y aurait un changement au bout d'un certain temps. C'est là la raison de ce changement, non pas parce qu'il y a eu un problème.

WES HARDAKER : Oui, un autre commentaire. Du point de vue opérationnel, c'est une bonne idée de changer les clés même si vous n'avez pas de problème. C'est juste pour s'assurer que tout le monde peut prendre la clé et il vaut mieux le faire lorsqu'il n'y aura pas de problème parce que s'il faut vous lancer dans ce processus et que vous ne l'avez jamais fait auparavant, il est fort probable que vous vous trompiez. Donc la génération de la nouvelle clé, c'est ce qui s'est passé en février, le changement vers la nouvelle clé était censée avoir lieu en octobre. Et en raison du fait qu'on était en train de voir si les gens ont utilisé plutôt l'ancienne clé ou la nouvelle clé, il y avait encore beaucoup de gens qui n'avaient pas commencé à valider la nouvelle clé encore. Donc l'ICANN a décidé de reporter cela et il y a eu un appel à contribution de la communauté pour voir si on attendait jusqu'au mois d'octobre prochain. Et il est important de bien comprendre cela et de bien comprendre pourquoi on veut une nouvelle clé. Et donc je vous le disais, cette période de

commentaires publics est ouverte encore jusqu'au 3 avril je crois.

Autres questions dans la salle ? Une question encore.

ABDALMONEM GALILA : Avec quelle fréquence le roulement KSK va avoir lieu ?

WES HARDAKER : Combien de temps cela va prendre ou avec quelle fréquence ?

ABDALMONEM GALILA : Combien de temps cela va prendre.

WES HARDAKER : Alors à l'origine, cela a été conçu pour être fait en cinq mois, c'est cela ?

ORATEUR NON-IDENTIFIÉ : Oui, la question portait sur la fréquence, à quelle fréquence on a le roulement KSK.

WES HARDAKER : Cela, c'est sujet à débat. Je pense que les politiques publiées par l'ICANN stipulent qu'il faut le faire tous les cinq ans maintenant. Alors savoir si on va attendre cinq ans ou pas, je pense qu'une

fois que le roulement actuel sera fait, on va voir si on a besoin d'une fréquence plus régulière. Mais je pense que cette politique va être révisée de nouveau.

Oui, rapidement s'il vous plaît.

ABDALMONEM GALILA : Dernière question. Est-ce que l'ICANN a une garantie pour faire la validation DNSSEC pour qu'il y ait roulement KSK depuis la zone racine ?

WES HARDAKER : Personne n'a autorité sur tous les FSI du monde. Donc la réponse est non, c'est impossible. En théorie, les gouvernements pourraient le faire mais aucun gouvernement n'a essayé de mandater les FSI pour qu'ils le fassent. Mais bonne question.

Bien. Merci à tous d'être venus. On n'a plus de temps. Merci à tous, excellentes questions. Et j'espère que vous ressortez de cette salle en ayant appris beaucoup de choses.

[FIN DE LA TRANSCRIPTION]