COPENHAGUE – Les DNSSEC pour tous : Guide du débutant
Dimanche 12 mars 2017 – 17 h à 18 h 30 CET
ICANN58 | Copenhague, Danemark

WES HARDAKER : … séance, et ce qu'on fait pour vous, et dans quelle mesure ça protège votre infrastructure, votre nom de domaine. On va donc entrer dans le détail de tout cela, mais d'abord, une petite histoire.

Certains disent que le DNSSEC date de 5000 ans avant Jésus Christ. Partons de cette idée. Alors, on va voir un certain nombre de personnages.

D'abord, Ugwina, qui vit dans une grotte, une grotte au bord du Grand Canyon. Et voici Og, qui vit aussi dans une grotte, mais de l'autre côté du Grand Canyon, de l'autre côté.

C'est donc difficile pour eux de communiquer parce qu'il faut descendre, contourner et Og et Ugwina ne peuvent pas se parler très souvent. Lors de l'une de leurs rares rencontres, ils voient de la fumée émanant du feu, et qu'ils peuvent utiliser cette fumée pour communiquer.

C’est un peu ça, le DNS. Il y a le client à distance qui vous pose une question et vous pouvez répondre grâce à ces signaux de fumée.

Donc, un jour, il y a un méchant homme des grottes, Kaminsky, qui a trouvé un trou, un grand trou dans le DNS et qui s’installe dans la grotte à côté de Og et qui se met, lui aussi, à envoyer des signaux de fumée.

Et maintenant, Ugwina est réellement perturbée. Elle voit deux signaux de fumée et ne sait pas lequel croire. Elle voit un signal qui lui dit « je t’aime beaucoup, Ugwina » et un autre qui lui dit « je ne t’aime pas du tout, Ugwina ». Lequel croire ?

Donc, Ugwina descend de sa grotte pour essayer de résoudre ce problème, et Ugwina et Og vont consulter les anciens, l’homme des grottes Diffie, pour lui poser la question et voir s’il a une idée brillante. Et en un éclair, l’ancien rentre dans la grotte de Og et trouve une montagne de poudre bleue qui existe uniquement dans la grotte de Og.

Elle lance cette poudre bleue sur le feu de Og et s’aperçoit que ça peut les aider, parce que maintenant, lorsque Ugwina et Og veulent communiquer, il va falloir qu’elle fasse confiance uniquement à la fumée bleue, et plus aux signaux de fumée blancs du méchant Kaminsky.

Voilà un peu l'histoire derrière cette anecdote du DNSSEC qui date d'il y a 5000 ans.

Si vous ne connaissez pas bien le DNS, sachez que l'idée principale, c'est qu'il y a une arborescence. Ce qui se passe, c'est que les résolveurs répondent à une question en commençant tout en haut, à la racine, et la racine répond à UK, COM, etc. Chacun a un sous-groupe. CO.UK, BIGBANK.COM. Donc c'est une arborescence. On va y revenir dans un instant.

Comme je vous le disais, le résolveur connaît le chemin en essayant de trouver une réponse pour vous, lorsque vous tapez un nom de domaine et chaque niveau vous fait passer au niveau suivant jusqu'à ce que vous obteniez une réponse à votre question.

L'un des avantages, c'est que le résolveur contient ces informations pour faire en sorte que vous puissiez obtenir une réponse immédiate, sans avoir à revenir en arrière dans le processus.

Le problème, c'est que, et ça c'est l'idée principale du DNS seul, sans le DNSSEC, parce que si le DNS résout le problème, c'est qu'il n'y a pas de sécurité, pas de garantie pensée à cette image de la fumée bleue par rapport à la fumée blanche. Sans cette fumée bleue, vous ne pouvez pas être sûr que la réponse est bonne.

Donc les noms sont facilement usurpés, et lorsque vous avez des caches, vous pouvez obtenir la mauvaise réponse derrière ces caches qui sont, eux aussi, facilement usurpés.

Pour illustrer cette idée, on va vous faire un petit sketch. Je vais demander à nos acteurs principaux de bien vouloir se lever. On peut faire une rangée ici. Chers collègues, malheureusement certains acteurs sont malades, donc je vais improviser et participer moi aussi à ce petit sketch.

Alors moi, je serai l'utilisateur sur Internet, l'utilisateur Joe qui veut faire une opération bancaire aujourd'hui.

Vous ne me croiriez pas si je vous disais combien de fois on a mis ces t-shirts.

Bien. Donc je suis l'utilisateur Joe et je vous présente monsieur fournisseur de services Internet. C'est à lui qu'il faut s'adresser en premier si vous avez besoin d'un service Internet.

Ensuite, Bigbank.com qui connaît toutes les informations bancaires.

Com sait où se trouve bank.

Puis la racine, qui est la source de tout. La racine sait où se trouve com et tout le reste.

Alors, je vais sur mon ordinateur, je veux faire des opérations bancaires, je me connecte et je dis « je veux aller sur bigbank.com » et j'attends que le DNS réponde.

WARREN KUMARI / FSI : Alors, vous voulez savoir où se trouve Bigbank ?

Très bien. Bonjour, Racine, mon utilisateur voudrait aller sur www.bigbank.com. Où est-ce ?

KATHY SCHNITT/RACINE : Ah, bonjour. Je ne sais pas où ça se trouve Bigbank.com mais je peux te dire où est .com. 1.1.1.1.

WARREN KUMARI/ FSI : Super, merci.

Bonjour, .com. Je suis FSI, et un de mes utilisateurs veut aller sur www.bigbank.com.

JACQUES LATOUR/ .COM : Je suis désolé, je ne sais pas où c'est mais je sais que Bigbank est à 2.2.2.

WES HARDAKER/ FSI : Très bien, merci. Bonjour Bigbank, l'un de mes utilisateurs veut aller sur ton site, où se trouve www.bigbank.com ?

IRWIN LANSING/ BIG BANK : Attends une seconde, laisse-moi vérifier. C'est à 2.2.2.3.

WARREN KUMARI /FSI : Très bien, mon utilisateur va être ravi.

Voilà, cher utilisateur, 2.2.23.

WES HARDAKER/JOE : Parfait. Maintenant, mon navigateur peut y aller, je regarde mon compte et j'ai 2 millions de dollars sur mon compte. Comment utiliser cet argent à bon escient ?

C'est comme ça que fonctionne le DNS en l'absence de problèmes.

Alors vous vous souviendrez que le résolveur Ugwina est en train de chatter avec les serveurs. Avant, elle était perdue, jusqu'à cette poudre dans la fumée.

Maintenant, on va vous montrer comment le DNSSEC peut résoudre la situation lorsqu'elle se complique.

Imaginez lorsqu'on vous donner deux réponses, une bonne et une mauvaise. Le problème avec le DNS, c'est que vous allez croire la première réponse que vous obtiendrez.

Le DNSSEC permet de résoudre cela en donnant les signatures de cryptographie bleue, de la fumée bleue pour s'assurer que les informations sont correctes et parviennent au bon endroit. Donc les signatures sont utilisées pour s'assurer que tout ce qui est stocké dans le DNS est parfait et n'a pas été modifié depuis la publication par son éditeur. Ça peut être utilisé par le serveur ou par n'importe qui.

Le DNS est un système de recherche, donc vous pouvez chercher d'autres choses. Les clefs cryptographiques sont stockées dans le DNS également. Le résolveur a seulement besoin de connaître la clef d'un serveur.

Kathy, la racine, si vous connaissez cette clef, vous connaissez celles de tout le reste. Vous n'avez pas besoin de mémoriser toutes les autres clefs, ce qui permet de constituer une chaîne de confiance. La clef vous amène à un autre niveau, puis à un autre, etc.

Ce qu'on essaie de voir, ici, vous pouvez voir les encadrés cochés, vous êtes sûrs d'être parvenus au bon endroit, et en rouge, c'est la mauvaise réponse.

Revenons à notre petit sketch.

J'essaie de me connecter pour des opérations bancaires. Voyons, j'ai décidé avec mes millions de dollars de consacrer des milliers de dollars à l'achat d'un nouvel ordinateur.

WARREN KUMARI / FSI : Si vous avez des millions de dollars, je pense qu'on peut augmenter nos tarifs en tant que fournisseur Internet.

Bonjour, racine. L'un de mes utilisateurs veut aller sur www.bigbank.com. Où est-ce ?

KATHY SCHNITT/ RACINE : Bonjour, FSI. On devient véritablement amis, dis donc.

Désolée, je ne sais pas où c'est. Je ne sais pas où se trouve bigbank.com, mais je sais où se trouve .com. 1.1.1.1.

WARREN KUMARI/ FSI : Très bien.

Alors, .com, l'un de mes utilisateurs aimerait aller sur www.bigbank.com.

JACQUES LATOUR/ .COM : Là on a un problème de mémoire. Je ne sais pas où se trouve bigbank.com, mais je sais où se trouve Bigbank. C'est 2.2.2.

WARREN KUMARI/FSI : Bon, je vais demander aux serveurs.

Bonjour, Bigbank. Où se trouve www.bigbank.com ?

MÉCHANT : Oui, bien sûr, vous pouvez trouver www.bigbank.com sur 6.6.6.6.

WARREN KUMARI/ FSI : Très bien, merci pour cette réponse rapide. D'ailleurs, vous avez un bien meilleur aspect que le serveur précédent.

Alors voici la réponse.

WES HARDAKER/JOE : Merci beaucoup... Mais ?! Où s'est évaporé mon argent ??

Vous voyez le problème. Vous avez cru la première personne à vous donner une réponse. On est actuellement exactement dans la même situation, mais avec le DNSSEC, je vais demander à mon FSI où se trouve www.bigbank.com.

Monsieur FSI ?

Ne croyez pas qu'on improvise, on a répété plusieurs fois.

Excusez-moi, monsieur FSI, où se trouve www.bigbank.com ?

WARREN KUWARI/ FSI : Je vais aller vérifier.

Bonjour, .com, vous vous souvenez de moi ? L'un de mes utilisateurs veut aller sur www.bigbank.com. J'ai la mémoire qui flanche, où est-ce que ça se trouve ?

KATHY SCHNITT/ RACINE : Votre utilisateur utilise trop les services bancaires. Je ne sais pas où se trouve www.bigbank.com mais je sais où se trouve .com. 1.1.1.1.

Mais avant que vous ne vous y rendiez, je crois que je devrais signer ce papier.

WARREN KUMARI / FSI : Attendez une seconde. Oui, oui, ça ressemble à votre signature, je vous crois.

Bonjour, .com. L'un de mes utilisateurs aimerait aller sur www.bigbank.com. Où est-ce ?

JACQUES LATOUR/ .COM : Désolé, je ne sais pas où se trouve www.bigbank.com, mais je sais où se trouve Bigbank. Ici, 2.2.2.2.

WARREN KUMARI/ FSI : Voulez-vous bien signer ici pour que je puisse comparer ?

Oui, ça ressemble à votre signature. Je vais donc demander à 2.2.2.2.

Bonjour, pouvez-vous me dire où se trouve www.bigbank.com ?

MÉCHANT : Vous pouvez trouver www.bigbank.com sur 6.6.6.6.

WARREN KUMARI/ FSI : Attendez un instant là, cette signature n'est pas bonne, je ne vous crois pas.

Bonjour, Bigbank, pouvez-vous me dire où se trouve www.bigbank.com ?

IRWIN LANSING/ BIG BANK : Bien sûr, avec grand plaisir. C'est sur 2.2.2.3. Et voilà ma signature.

WARREN KUMARI/ FSI : Oui, c'est la même signature donc je vais faire confiance à ce serveur là.

Voici, monsieur l'utilisateur, 2.2.2.3 et je l'ai vérifié.

WES HARDAKER/ JOE : Alors cette fois-ci, mon argent est sur mon compte.

Voilà donc comment ça fonctionne. On applaudit bien fort nos acteurs.

Maintenant, on va retirer nos t-shirts.

Bien. J'espère que vous avez pu avoir un aperçu général de ce qu'est le DNSSEC et si vous retenez et comprenez cette idée, c'est déjà essentiel, parce que c'est fondamentalement comme ça que ça marche. Vous pouvez recevoir des réponses sécurisées.

Alors voici un exemple expliquant pourquoi vous avez besoin du DNSSEC et un guide simple pour le déployer.

Pourquoi se préoccuper du DNS ? Les utilisateurs pensent en termes de noms. On les utilise depuis la naissance de l'Internet, et les candidatures aussi utilisent les noms. Lorsque vous cherchez des informations sur les noms, mais aussi des informations pour les images, les encryptages, etc. On aura une diapo plus détaillée là-dessus un peu plus tard.

Mais Internet utilise des adresses et non pas des noms. À partir de là, vous utilisez des adresses IP, IPv4, IPv6, et le DNS fournit

un peu la colle pour vous permettre d'effectuer ce que le DNS est censé effectuer. Il y a des demandes sur pratiquement tout. Tout passe par le DNS. C'est une composante essentielle du fonctionnement de l'Internet.

Le problème, c'est qu'il peut y avoir du piratage. C'est ce qu'on a vu dans le sketch. Avec une réponse erronée mais plus rapide, vous obtenez ce genre de problèmes. Ce qui se produit, c'est que les utilisateurs peuvent être redirigés vers un autre site Web, vers une autre adresse IP hébergeant les mêmes éléments mais vous vous apercevez que votre mot de passe vient d'être usurpé. Ça c'est l'attaque de l'homme intermédiaire.

Si vous vous regardez un peu ce qui se passe actuellement, vous vous apercevrez que c'est quelque chose de très courant. Dans certaines universités, on forme les étudiants à créer des logiciels de piratage du DNS.

Le DNSSEC, c'est un peu une garantie, c'est le sticker sur les cartes et c'est ce qui vous garantit que vous allez au bon endroit et ça améliore en cryptant afin que vous obteniez les données du système créées par la personne qui en est à l'origine.

Donc, les personnes qui ont créé les données, quelle que soit la distribution de ces données, ce pourrait être sur un papier envoyé dans la salle, vous pourriez vérifier la signature.

Donc, l'exemple de piratage qu'on vient de voir vous montre où se situe le problème, mais on a d'autres exemples. Vous voyez ici un diagramme de situations comparables.

Je ne vais pas entrer dans le détail, mais c'est un peu le même cas de figure. Nous avons un serveur de nom faisant autorité, un serveur Web, un serveur de nom récursif et Joe l'utilisateur ici, donc un peu le même diagramme que la situation que nous avons vue sous forme de sketch. Il peut y avoir plusieurs serveurs de nom récursif, un serveur Web, un serveur de nom faisant autorité, etc., mais c'est le même cas de figure. N'appuyez pas sur le mauvais bouton. Ça, c'est ce que j'ai appris dans la vie.

Ce qui se produit, c'est que l'utilisateur envoie la demande et l'envoie à son FSI. Le résolveur récursif l'envoie au serveur de noms faisant autorité, qui l'envoie en retour au serveur de nom récursif qui, à son tour, vous l'a renvoie. C'est clair, vous avez une question et quelqu'un y répond. Vous vous adressez donc à plusieurs personnes, comme on l'a vu pendant le sketch. Donc finalement, l'utilisateur d'adresse à la bonne personne.

Lorsque je travaillais à Parsons, on avait retiré le navigateur Firefox pour faire de la validation DNSSEC et vous voyez ici sur cette diapo, vous voyez ici cette case cochée DNSSEC. Si vous utilisez un navigateur de validation ou un fournisseur de service

Internet validé, vous verrez cette marque cochée en vert. Si vous n'avez pas d'environnement de validation, vous verrez ce signal d'alerte qui vous dit « DNSSEC is off ».

Donc, pour revenir à l'exemple du piratage, nous avons un méchant qui se trouve ici, en bas. L'utilisateur envoie donc la demande au serveur récursif, mais le méchant est juste à côté de lui et peut donc répondre très rapidement, beaucoup plus vite que le FSI. Il lui dit « écoutez, j'en ai rien à faire de votre côté, moi je vais vous envoyer la mauvaise réponse ».

Ce qui se passe, c'est que l'utilisateur Joe est redirigé vers un autre site Web que le méchant peut contrôler. Ça montre un peu que les autres informations continuent de circuler et reviennent vers Joe l'utilisateur, mais trop tard.

Donc, le DNSSEC consiste justement à stopper ça, le fait que quelqu'un pirate cette information, à s'assurer que les informations sont envoyées à la bonne personne et qu'elles sont correctes.

Ce n'est pas ma présentation donc je ne sais plus où ont lieu les animations. Moi, je suis remplaçant mais je connais bien cette présentation.

Pour revenir à cet exemple. Vous voyez ici la case cochée de confirmation verte. Pourquoi ? Parce qu'il y a eu contrôle DNSSEC, donc vous n'avez pas ce message « DNSSEC is off ».

Alors, un point important dont peu de gens ont conscience. Si vous allez sur CNN.COM, savez-vous combien de recherches DNS pour avoir accès à ce site Web ?

Énormément. Il y a 5 ou 10 ans, je travaillais pour Parsons et je leur montrais toutes les requêtes pour avoir accès à CNN.COM. Toutes ces lignes bleues et vertes, ce sont celles qui correspondent à une requête pour un seul site Web. Là, vous voyez un autre exemple de la même chose, vu différemment.

Toutes ces lignes sont très belles, mais imaginez à quel point, pour les experts, c'est difficile d'avancer dans cet environnement. Vous voyez ici tous les liens Google, etc., qui arrivent tous au même point.

Il existe certaines fonctions du DNS qui sont fondamentales. Ce n'est pas une seule personne qui fait tout cela. En fin de compte, ce sont les données qui sont importantes. Il faut protéger les donnés. Quelles que soient les personnes impliquées, du moment qu'il y a signature, c'est bon.

Voici une illustration de la complexité de tous ces processus. Nous avons ici, en haut à gauche, une requête. J'ai besoin

d'avoir un enregistrement, j'envoie cette requête à la zone, au serveur faisant autorité, serveur récursif et le client pose, lui, des questions, au serveur récursif. On va revoir ce diagramme avec l'ajout du DNSSEC.

La mise en œuvre du DNSSEC dépend surtout des mêmes éléments, on a ajouté des informations. Le DNSSEC est constitué de plusieurs éléments et il y a des activités avec différentes fonctions complexes du DNS et des activités de mise en œuvre plus complexes relatives au DNSSEC. Si les choses sont simplement mises en œuvre, c'est plus facile de déployer le DNSSEC.

Quelques exemples. Un opérateur de registres responsable d'une opération TLD de grande envergure, par exemple .COM, c'est probablement plus difficile que pour n'importe quelle autre personne. Une grande entreprise aussi, avec beaucoup de services qui changent régulièrement, par exemple HP.COM. Les entreprises basées sur l'Internet, avec des zones commerciales critiques. Eux consacrent énormément de temps à voir quand les choses se compliquent.

Si quelqu'un pirate votre zone, vous ne le saurez probablement pas parce qu'il y a des efforts pour superviser et surveiller tout cela.

Ensuite, il y a des activités avec des zones non-critiques du DNS, donc c'est moins critique mais c'est un projet open source, ce n'est pas une banque mais c'est quelque chose d'intéressant, de très important. Vous avez, par exemple, des images qui correspondent à des photos de votre famille ou des choses personnelles de ce genre.

Donc, le DNSSEC est nécessaire pour éviter les attaques vis-à-vis du contenu DNS, mais ça marche lorsque vous protégez vos données de zone. Si ce n'est pas le cas, le DNSSEC ne vous aidera pas parce que vous n'avez pas protégé votre base de données, donc assurez-vous que vous protégez vos données de zone. Ça ne règlera pas vos autres problèmes de piratage des serveurs.

Pour revenir à ce diagramme, on a ajouté quelques autres éléments en ajoutant le DNSSEC. Maintenant, il y a des données signées.

Alors, on va d'abord signer les données avant de les envoyer au serveur faisant autorité. Ensuite, les clefs cryptographiques doivent être signées entre les données signées et le serveur récursif. Le seul symbole de verrouillage, c'est entre les données signées et le serveur récursif.

Si vous avez un réseau très actif, vous devrez consacrer plus d'énergie pour le conserver, ainsi que pour vous protéger grâce

au DNSSEC. Donc si vous faites des choses moins importantes, ça marchera et si vous faites des opérations beaucoup plus complexes, vous aurez alors besoin d'un niveau de DNSSEC plus complexe aussi.

Sur ce, on va faire une petite pause pour écouter vos questions, voir si vous avez des questions, donc, sur le DNS ou le DNSSEC.

Est-ce que Matt Larson est là ? Je vais lui donner cinq minutes pour qu'il puisse nous parler un peu. Matt Larson va parler de la signature de clef, donc du roulement de clefs. Je ne sais pas si vous avez vu le dernier diagramme mais en fait, il faut que les FAI connaissent le transfert qui se fait, donc Matt va nous en parler.

MATT LARSON : Bonjour à tous. Je m'appelle Matt Larson, je suis vice-président de la Recherche dans le Bureau Technologique de l'ICANN. Je suis donc l'une des personnes impliquées dans le projet de roulement de la zone racine, le KSK.

Ça, c'est ce qu'on a créé en 2010 lorsqu'on a créé la racine pour la première fois et cette clef n'a pas changé depuis, c'est toujours resté la même. L'idée n'était pas qu'elle reste la même et dans certains des documents que nous avions préparés, on s'était dit qu'on lancerait cette clef au bout de cinq ans. Cela fait

donc cinq ans et nous en sommes là. Je voulais donc vous dire un peu où nous en sommes de ce projet.

Alors, le projet, eh bien il va falloir un certain temps pour le mettre en place. Le changement se fera délibérément lentement. Nous ne sommes pas très pressés puisque nous sommes dans le cadre d'une opération tout à fait normale, il n'y a pas de problèmes que nous connaissions par rapport à la KSK actuelle donc nous pouvons procéder de manière délibérée et raisonnable.

Il y a certains délais, quand même. La nouvelle KSK a été créée en octobre dernier et l'ICANN utilise deux sites de stockage de la KSK, dans des lieux sécurisés. La clef a été créée sur un site et ensuite, elle a été emmenée vers l'autre site. Elle a été créée sur la côte Est et a été emmenée sur la côte Ouest.

Donc, une fois par trimestre, on vérifie que la KSK signe la ZSK. Le résultat, c'est qu'on a décidé de mettre tous les événements relatifs au KSK, donc ce rythme en fait. Au dernier trimestre de l'année dernière, on a créé la nouvelle clef et cette année, on l'a déplacée vers l'autre site, sur la côté Ouest des États-Unis. Une fois qu'on a eut stocké cette clef, on a obtenu deux sites et donc elle était opérationnelle.

Ensuite, l'étape la plus récente, ça a été la deuxième cérémonie de signature de clefs, Q2, où là nous avons publié la clef et

l'avons donc utilisée pour la première fois. La clef est donc disponible.

Elle apparaîtra dans le DNS en juillet et le 11 octobre 2017 est normalement la date. Je sais que c'est en caractères gras, donc le 11 octobre 2017 est la date à connaître. Nous arrêterons d'utiliser la KSK actuelle et utiliserons la nouvelle. Nous l'appelons KSK 2017, l'ancienne était la KSK2010.

Si vous utilisez un logiciel valide et configurée pour cette KSK, il va falloir changer vos informations. Voilà pourquoi cette date est très importante. D'ici le 11 octobre, toute validation du DNSSEC avec un logiciel configurée avec l'ancienne KSK devra passer à la nouvelle KSK.

Il y a beaucoup d'informations sur cette URL qui donne des informations continuellement, au fur et à mesure des mises à jour, sur la KSK et vous pouvez y obtenir des liens.

Alors, ma présentation a été très rapide parce que je ne savais pas que j'aurai tout ce temps, mais de toute façon, je présenterai de nouveau ces informations lors d'une autre séance. Lors des autres réunions DNSSEC, je serai présent, d'autres personnes seront là et pourront entrer dans le détail.

Je ne sais pas s'il y a des questions. Est-ce que je peux demander s'il y a des questions ?

WES HARDAKER : Restez-là. Nous avons des experts qui vont vous rejoindre donc n'importe qui pourra répondre aux questions parmi les experts. Nous allons donc effectivement passer à vos questions pour le reste de notre séance. Je ne sais pas par quoi vous voulez commencer.

Que veut dire DNSSEC ? Matt a parlé des clefs, de clefs de DNSSEC ? Si on rentre dans la complexité, on pourra en apprendre davantage sur ces différentes clefs.

Mais oui, effectivement, on va poser des questions et demander à nos experts de répondre.

MICHAEL OGHIA : Bonjour, je m'appelle Michael Oghia, c'est la première fois que je viens à une réunion ICANN. Je suis également boursier pour la première fois.

J'ai plusieurs questions sur le DNSSEC. De toute évidence, pour certains ce seront des questions élémentaires, mais j'aimerais en savoir plus.

WES HARDAKER : Oui, ce n'est pas grave. C'est une bonne chose de poser des questions.

MICHAEL OGHIA : Comment certains outils comme le DNSSEC ou le https se complémentent les uns les autres ? Le https c'est au niveau de l'application et le DNSSEC au niveau du protocole, mais ce que j'aimerais savoir, c'est comment tout ceci créé une suite d'utilisation tout ensemble pour les utilisateurs.

J'ai une autre question – je ne sais pas si...

WES HARDAKER : On va d'abord répondre à cette question.

Jacques, c'est à vous de répondre, allez-y.

JACQUES LATOUR : Au niveau du DNS, le DNSSEC, c'est l'intégrité du DNS. L'idée est de conduire au bon serveur lorsqu'on entre un nom de domaine, qu'on arrive à la bonne adresse IP, qu'elle soit valide. Donc, le DNNSEC n'a rien à voir avec ce que fait le https. Voilà pour la première partie.

MICHAEL OGHIA : D'accord. Alors, pourquoi est-e que j'ai besoin du DNSSEC si j'ai le https ?

JACQUES LATOUR : Peut-être que quelqu'un d'autre peut répondre à ça.

WARREN KUMARI : Il semblerait que si on le https, il n'est pas aussi important que ça d'avoir le DNSSEC, parce que normalement on devrait avoir le bon certificat. Malheureusement, cela ne fonctionne pas dans tous les cas. Dans certains cas, on arrive à des sites ayant des certificats mais étant des sites de hackers, de pirates.

Par ailleurs, si on n'a pas le DNSSEC, l'attaquant peut continuer de vous soumettre des sites et c'est un problème de DOS.

Le DNSSEC vous permet également de faire d'autres choses qui ne sont pas mal. On peut bâtir d'autres choses sur la base du DNSSEC. On peut donc l'utiliser comme protocole de base pour ajouter d'autres choses.

Et ce n'est pas du tout une question stupide, beaucoup de gens se la posent, en fait.

MICHAEL OGHIA : Merci. D'accord, je comprends mieux la différence par rapport aux données envoyées sur un site Web en passant pas un canal https crypté alors que le site initial que l'on me montre, en tant qu'utilisateur final, pourrait être, en fait, un site malveillant.

WES HARDAKER : Oui, c'est une question de couches. Si vous êtes déjà au mauvais endroit, on ne peut pas avoir de sécurité. Alors que par le routage, vous avez les applications donc, tout à fait, c'est complexe.

Deuxième question, allez-y.

MICHAEL OGHIA : Et puis bien sûr que l'attaquant peut avoir un site crypté.

Deuxième question, maintenant. Pourquoi tous les bureaux d'enregistrement ne proposent pas le DNSSEC pour chaque – comment dire – chaque TLD ? Parce que, par exemple, moi j'ai une adresse .ORG et mon bureau d'enregistrement ne propose pas le DNSSEC pour ça. Moi, je voudrais payer pour l'avoir, et je ne comprends pas pourquoi ils ne le proposent pas.

WARREN KUMARI : Je ne comprends pas non plus. Vous pouvez simplement changer de bureau d'enregistrement. Je pense que la plupart d'entre eux le proposent et je suis tout à fait d'accord avec vous que ce devrait être proposé.

CHRISTIAN HESSELMAN : Au début, en fait, la technologie n'était pas bien connue. Ils ne la connaissaient pas bien, et donc pour eux, ça voulait dire une

mise à jour de leur infrastructure et il fallait qu'ils en voient les avantages. Vous êtes en fait l'un des premières personnes qui posent cette question d'avoir un domaine signé par le DNSSEC, parce qu'en général, les utilisateurs finaux ne savent même pas à quoi ça correspond le DNSSEC. Ils tapent leur nom de domaine et point final.

En fait, c'est une question d'infrastructure qui doit être mise en place chez les bureaux d'enregistrement, et si les consommateurs ne le demandent pas, ils ne le font pas. Donc de nombreux opérateurs de registre de ccTLDs essaient, en principe, de motiver leur bureau d'enregistrement pour qu'ils passent à la signature DNSSEC. Soit en utilisant des programmes de motivation, soit en les éduquant, ça peut être financier aussi, en général.

MICHAEL OGHIA : Oui, justement. J'ai eu justement cette discussion lors d'une autre réunion et c'est également l'aspect financier. Le manque de clients qui souhaitaient le DNSSEC. Donc, je crois que je vais commencer à envoyer des emails à mon bureau d'enregistrement pour lui demander de le proposer pour le .ORG.

WES HARDAKER : Oui, je le recommande, parce que pour certains, c'est très simple, il suffit de cocher et c'est terminé. En tout cas, c'est tout à fait bénéfique.

Alors, il y a une question en ligne, et je crois qu'il y en avait une autre, une ou deux là-bas. On va d'abord commencer par la question en ligne.

JULIE HEDLUND : Merci beaucoup, Wes. La question est la suivante, et nous vient d'Alexandrine Gauvin : « Est-ce que le DNSSEC doit être activé à tous les niveaux - FSI, TLD, navigateur, logiciel, etc. – pour pouvoir fonctionner ?

WES HARDAKER : Qui veut répondre ? Allez-y.

ERWIN LANSING : La réponse brève, c'est oui, au moins pour le DNS. Il faut une hiérarchie en partie de la racine jusqu'aux serveurs, tout doit être signé.

Sans vouloir entrer dans tous les détails, souvent, on se demande si on peut faire confiance à tout le chemin depuis le FSI jusqu'en haut, mais je crois qu'il y a quand même une chaîne qui doit fonctionner.

WARREN KUMARI : Oui, pour poursuivre là-dessus, je crois que tous les nouveaux gTLDs doivent être compatibles avec le DNSSEC, et la plupart des TLDs également. Presque tous les bureaux d'enregistrement, mais pas tous. Beaucoup de résolveurs, aussi. Le Google Public DNS aussi. Beaucoup d'entre eux ont donc une validation DNS.

Je ne sais pas si Geoff Houston est là, mais il a fait certaines expériences qui montrent que 15% de toutes les requêtes sont protégées par le DNSSEC.

Par rapport aux résolveurs, ça ne vous protège pas nécessairement. Il faut donc un moyen de l'installer sur votre machine en toute sécurité, ce qui veut dire que la machine doit faire sa propre validation. C'est la meilleure option. C'est quelque chose que vous pouvez faire. Vous avez des logiciels permettant ça, il y a des navigateurs également qui effectuent la validation du DNSSEC – il y a [Bloodhound], Fork. Il y a des extensions que vous pouvez ajouter aux navigateurs aussi, pour savoir si la validation DNSSEC a été faite.

WES HARDAKER : En fait, c'est un processus. Tout ce qui est lancé tôt est protégé tôt. Donc, ce n'est pas comme si la totalité de l'arbre était

signée. Il faut aller chercher dans le détail un peu. Donc, si vous signez votre zone et que vous vous enregistrez avec un TLD parent signé, à ce moment-là, vous avez protégé vos données. Si votre concurrent ne le fait pas, c'est son problème.

Actuellement, je crois que nous avons 0,5% des zones .COM qui sont signées. Ça peut sembler minuscule comme pourcentage, mais je crois que ça fait 500 000 domaines du .COM qui ont été signés, ce qui n'est quand même pas mal. On voit que ça commence à prendre.

WARREN KUMARI : Pour poursuivre, il y a des TLDs qui demandaient le DNSSEC, je crois que c'étaient .BANK et .INSURANCE, qui voulaient que tous les noms de domaine soient signés par le DNSSEC. De toute évident, parce qu'il faut que ce soit très sécurisé pour les utilisateurs finaux.

WES HARDAKER : Autre question. Allez-y, monsieur.

CLÉMENT GENTY : Bonjour. Je m'appelle Clément, je suis en thèse de doctorant et je suis membre NextGen. Je crois que Jean-Jacques avait dit quelque chose comme quoi le DNSSEC était complètement invisible pour l'utilisateur final.

Alors, serait-il possible de demander à l'ICANN de demander aux bureaux d'enregistrement de proposer le DNSSEC pour tous les domaines ? Pourquoi est-ce que ce n'est pas une obligation d'avoir une sécurité d'une telle envergure avec le DNSSEC ?

WES HARDAKER : Matt, on vous envoie toutes les balles, toutes les balles sont dans votre camp.

MATT LARSON : Je voudrais m'assurer de bien avoir compris la question. Je n'ai pas entendu ce qu'a dit Jean-Jacques tout à l'heure. Le commentaire concerne la signature de domaine ? Ou bien ça concerne la possibilité de voir le statut de validation pour toutes les applications ?

WES HARDAKER: En fait, pourquoi est-ce que l'ICANN n'en demande pas plus aux bureaux d'enregistrement ? C'est ça la question, monsieur ?

CLÉMENT GENTY : Alors, si je veux résumer : pourquoi doit-on payer pour le DNSSEC ? Pourquoi n'est-il pas tout simplement disponible ?

MATT LARSON : Effectivement, vous m'attaquez, là. L'ICANN existe depuis beaucoup plus longtemps que le déploiement du DNSSEC donc les accords gouvernant la relation entre les opérateurs de registres, les bureaux d'enregistrements et l'ICANN sont antérieurs à ce que nous avons avec le DNSSEC actuellement.

Donc, l'ICANN a essayé de pousser le DNSSEC en disant, justement, que tous les nouveaux gTLDS doivent avoir le DNSSEC. Mais je crois que certains aspects, par exemple par rapport au modèle de travail des bureaux d'enregistrement, il y a différentes approches en termes d'accréditation et de vente de noms de domaine.

Je crois donc que c'est un secteur qui n'a pas été spécifié, qui n'a pas été détaillé sur le marché par l'ICANN.

WES HARDAKER : De nombreux accords existent entre les gouvernements et les entités commerciales, par exemple, entre différents organes. Il y a beaucoup de choses préexistantes et qui n'ont pas à appliquer les nouvelles règles.

Les nouveaux gTLDs sont obligés parce qu'ils sont par tout le processus de documentation et en plus, ils tombent dans le domaine des gouvernements. Lorsqu'on lance de nouvelles

initiatives, de plus en plus, on l'imposera. Il y a un processus de lancement qui doit être mis en place d'abord.

SALVINALE SU : Bonjour. Je m'appelle Salvinale Su et je suis entièrement nouveau ici. J'ai mon petit ruban vert de nouveau. Je fais partie de l'Internet Society, du chapitre de la Norvège.

J'aimerais que vous me donniez de petits conseils par rapport à mon chapitre. Que pourrait-on faire pour augmenter la visibilité du DNSSEC ? Que dois-je faire, moi, en tant que membre de l'Internet Society ? Avez-vous des idées ?

MATT LARSON : Le roulement de clefs doit être mentionné, c'est important pour moi, et je vous encourage vraiment en ce sens.

Pour tous ceux qui ne connaissent pas les différentes présentations faites par moi-même et mes collègues, le but est de s'assurer que cette date du 11 octobre 2017, à laquelle il faut absolument savoir que le KSK sera configuré.

C'est important, c'est quelque chose qu'on cherche à faire par le biais de présentations comme celle-ci, communiquer ce message à tout le monde.

WES HARDAKER : Jacques ?

JACQUES LATOUR : Une des ressources, c'est l'ISOC, qui a un programme déployé et une section sur le DNSSEC incluant de nombreux documents. Nous avons préparé pendant longtemps avec l'ISOC pour que les débutants comprennent les bases du DNSSEC, l'application, les FSI, les TLDs, etc., dans les différentes régions.

Dan York, qui est celui à contacter, a passé beaucoup de temps à rassembler toutes ces informations. Ça, c'est pour le DNSSEC.

Également, il y a les IPv6, ce qui est une nouvelle assez ancienne, et néanmoins une nouvelle nouveauté. Ce sont un peu les mêmes difficultés. L'ICANN ne peut pas forcer les gens à utiliser le DNSSEC et les IPv6, elle ne peut que le recommander sans pouvoir obliger. C'est un des problèmes et un des enjeux.

WARREN KUMARI : Je voudrais poursuivre là-dessus, l'Internet Society a fait un excellent travail de publicité sur le DNSSEC jusqu'à présent. Il y a Dan et d'autres. Un des premiers TLDs signés l'a été grâce à ça.

Ce que vous pouvez faire, c'est signer votre zone et parler à d'autres personnes. En fait, suggérer aux autres que c'est une bonne idée, expliquer quels sont les avantages, etc.

Je crois que Jacques a parlé d'IPv6, je crois qu'il y a 15% de DNSSEC et pour la v6, on est encore plus bas. Je crois donc que c'est important de parler de la v6 aussi.

WES HARDAKER : Avant de continuer, j'ai en fait oublié de présenter notre panel donc on va peut-être se présenter.

Moi, je m'appelle Wes [Hardaker], je fais partie de l'Université de Californie du Sud à l'ISI.

CHRISTIAN HESSELMAN : Je suis Christian Hesselman, de .NL, opérateur de registre pour les Pays-Bas.

JACQUES LATOUR : Jacques Latour, pour le Canada.

[ERWIN LANSING] : [Erwin Lansing, pour le Danemark.]

WARREN KUMARI : Warren Kumari, je travaille pour Google.

MATT LARSON : Matt Larson, ICANN.

WES HARADAKER : Julie, allez-y.

JULIE HEDLUND : Je ne suis pas experte, je fais partie du personnel de l'ICANN.

KATHY SCHNITT : Bonjour, je m'appelle Kathy et je suis également avec le personnel de l'ICANN.

WES HARDAKER : Merci beaucoup.

OLGA KYRYLIUK : Je viens d'Ukraine, et ma question peut sembler stupide, mais j'aimerais quand même que vous clarifiez quelque chose.

Si un bureau d'enregistrement n'active pas la vérification DNSSEC, l'utilisateur final n'a aucune possibilité de l'utiliser, c'est ça ? Donc, si je ne l'active pas sur mon navigateur également, dans ce cas-là, je ne verrai pas la petite case verte cochée, n'est-ce-pas ?

Si j'ai bien compris, 15% des bureaux d'enregistrement l'utilisent mais je ne l'ai jamais vue, moi, cette case verte. Cela veut-il dire que je dois l'avoir sur mon ordinateur ?

WES HARDAKER : Alors, c'est uniquement sur cette page Web, je clarifie. Ça, c'est quelque chose que nous avons fait pour dire aux gens de se rendre sur cette page Web. Peut-être que j'ai aussi créé la confusion parce que si votre FSI utilise la validation DNSSEC au niveau de son résolveur, vous voyez la case verte cochée. Ce n'est pas à vous de faire quoi que ce soit mais à votre FSI.

Matt ? Allez-y.

MATT LARSON : Je crois que ce qui est important, c'est de faire la distinction entre deux choses. À chaque fois que l'on parle de la DNSSEC, il ne faut pas oublier qu'il y a en fait deux parties majeures.

Il y a la signature, donc s'il y a des données DNS dont vous êtes responsable, si vous avez un domaine live sur l'Internet, il faut signer ces données. Ça, c'est l'aspect signature.

Et de l'autre côté, pour les recherches, pour ceux qui consultent ces données, c'est le côté validation. Donc, si on utilise un FSI avec validation de DNSSEC, à ce moment-là, on peut consommer les informations validées.

Mais les deux doivent fonctionner pour pouvoir utiliser véritablement le DNSSEC et en bénéficier. Si vous signez mais

que personne, de l'autre côté, ne valide, ce n'est que la moitié du travail qui est faite.

Donc, lorsqu'on parle des bureaux d'enregistrement, la question, c'est d'avoir la possibilité pour le détenteur de nom de domaine d'avoir des informations DNSSEC de manière à être signé, mais il existe aussi le côté validation. Les bureaux d'enregistrement ne sont, en principe, pas impliqués, c'est le travail des FSI.

CHRISTIAN HESSELMAN : Je suis d'accord.

WES HARDAKER : Autre question.

WARREN KUMARI : Je crois que vous avez parlé de l'Ukraine. [J'ai vérifié} les ccTLDs Ukraine. [J'ai vérifié et c'est bien signé].

CLAIRE CRAIG : Bonjour. Je m'appelle Claire Craig, je viens de Trinidad et Tobago et je fais des recherches dans le domaine des FSI. Je suis également membre de CaribNOGer.

Moi, ce qui m'inquiète un peu, c'est du point de vue des utilisateurs finaux, parce que vous savez, nous faisons tellement de choses pour que ceux qui ne sont pas connectés soient connectés, cela dit, très souvent les utilisateurs finaux se connectent et font des choses déraisonnables sur l'Internet.

Donc, en tant qu'utilisateur final, je ne veux pas nécessairement savoir ce que c'est le DNSSEC, peu importe, donc comment puis-je faire pour rester en sécurité sur l'Internet, pour ne pas courir de risques ? Comment est-ce que je peux obtenir des informations pour, par exemple, communiquer avec mon gouvernement, etc. ? Que dois-je savoir, en tant qu'utilisateur final, pour ne pas prendre de risques sur l'Internet ?

Parce qu'on dit aux gens ce qu'il faut faire sur les réseaux sociaux pour ne pas courir de risques, voilà maintenant la question que je vous pose.

WARREN KUMARI : Si votre FSI a le DNSSEC activé, peu importe, vous n'avez pas besoin de connaître le fonctionnement du DNSSEC, et si, par exemple, il y a eu piratage, vous n'arriverez pas à rejoindre ce site-là. Pour arriver à cela, demandez à votre FSI d'avoir une validation DNSSEC sur leur résolveur.

Cela ne veut pas dire que vous ne courrez aucun risque en ligne. C'est une partie de la réponse. De toute évidence, il ne faut pas cliquer n'importe où.

CLAIRE CRAIG : Oui, mais ce qui se passe, c'est que si je ne sais pas ce que fait le DNSSEC, je ne peux rien faire. Puis, il y a des FSI qui disent « on ne peut pas se le payer ». Il faut changer l'infrastructure, donc ça ne les intéresse pas.

Alors qu'est-ce que les utilisateurs doivent faire pour s'assurer que l'Internet ne les met pas en danger ?

MATT LARSON : Warren travaille pour Google donc il ne peut pas répondre à cette question, mais vous pouvez passer à un serveur récursif qui fonctionne avec le DNSSEC. Comme Warren l'a dit, il y en a d'autres. Il y a Google, il y a Verisign. Je ne les connais pas tous, mais c'est ça que peuvent faire les utilisateurs finaux.

Bien sûr, il faut penser aux configurations, connaître un peu le domaine, changer ce qui est par défaut. Donc, si les FSI peuvent activer la validation, c'est quand même mieux, mais les utilisateurs finaux peuvent quand même modifier certaines choses et ne pas nécessairement utiliser les serveurs récursifs par défaut.

WES HARDAKER : Pratiquement tous les opérateurs vous permettent de passer à un autre résolveur, mais de toute évidence, c'est un réglage un peu avancé.

WARREN KUMARI : J'ai regardé sur le site de Geoff Houston qui a fait un certain nombre de statistiques. Actuellement, 3,3% des gens font une validation DNSSEC [à Trinidad et Tobago].

WES HARDAKER : Allez-y, vous avez la parole.

SIMON SOHEL BAROI : Je m'appelle Simon Sohel Baroi, du Bangladesh. J'ai moi aussi une question stupide.

Cette année, les États-Unis ont un nouveau président, Président Trump, très bien. L'an dernier a eu lieu la transition IANA, très bien. Mais vous avez dit que les deux clefs se trouvent sur deux sites séparés mais toutes les deux aux États-Unis. Pourquoi pas dans une autre partie du monde ?

Ensuite, autre question stupide. Mon pays est un pays en voie de développement, c'est en tout cas ce que disent les Nations Unies. Dans ces pays, on voit ce genre de choses – le DNSSEC,

l'IPv6, le RPKI – et tous ces projets ne fonctionnent pas bien, en fait. Le DNSSEC a commencé il y a 10 ans. L'IPv6, c'était avant même que j'ai un ordinateur portable. Comment est-ce que ça se fait que ces projets ne soient pas développés plus vite ? On parle de 17% dans le monde, selon Geoff Houston. Pourquoi ?

MATT LARSON : Je crois que je vais répondre. Lorsqu'on a décidé, en 2010, de signer, à l'époque, il y avait encore un contrat entre l'ICANN et le département du commerce des États-Unis.

Pourquoi, sur un seul site, on a décidé de passer de la côte Est à la côte Ouest ? C'est ce qu'on a fait pour répondre à cette demande.

Vous avez mis le doigt sur un problème soulevé par d'autres avant vous, dans le cadre de la transition IANA. Pourquoi ne pas penser à un site en dehors des États-Unis ? Je pense que c'est une question tout à fait justifiée. Ça nous donnerait un tous une opportunité supplémentaire de partager un peu la responsabilité.

Cela étant dit, ce serait un changement très important que l'ICANN devrait organiser, important en termes de coûts aussi, et j'imagine qu'il y a beaucoup de pays qui aimeraient héberger cela. Cela dit, c'est quelque chose que l'ICANN en tant

qu'organisation doit commencer à entreprendre avec la communauté, parce que la communauté continue de dire que c'est un problème, mais il fait en faire une priorité que ces clefs soient gardées en dehors des États-Unis, ailleurs qu'aux États-Unis. Ce devrait être considéré comme une priorité devant d'autres priorités définies par la communauté.

JACQUES LATOUR : Moi, je vais répondre à la deuxième partie.

WARREN KUMARI : Les clefs sont toutes les deux aux États-Unis, toutefois, pour les utiliser, on a besoin d'un certain nombre d'éléments de la part du représentant habilité par la communauté, et donc de l'accord d'un certain nombre de pays pour éviter que des gens n'interviennent.

Donc, les clefs sont aux États-Unis, mais elles sont bien gardées et si quelqu'un essaie de les ouvrir, toutes sortes d'alarmes s'activent. Donc, c'est quelque chose de préoccupant mais moins qu'à première vue.

JACQUES LATOUR : Pour votre deuxième question. Pourquoi ça prend autant de temps ? L'IPv4 fonctionne depuis 35 ans maintenant, donc je pense qu'il est temps d'envisager sa retraite.

Le DNSSEC existe lui aussi depuis longtemps, et la raison pour laquelle c'est difficile d'avancer, c'est la résistance au changement.

Pour certaines raisons que j'ignore, on aime l'IPv4 et on aimerait qu'il dure encore plus longtemps. Donc, moi je suis favorable du retrait de l'IPv4 pour passer à l'IPv6.

On me dit « vous, vous dites qu'il faut clore l'IPv4 ». Il faut gérer ce changement au niveau mondial, ce qui est très difficile, ce qui explique qu'on soit confrontés à ce genre de problèmes.

CHRISTIAN HESSELMAN : Oui, il faudrait que ce soit une demande de la part du client. Ce n'est pas l'ICANN. C'est une actualisation d'infrastructure qu'il faut mettre en œuvre en tant que communauté.

Je voulais faire un deuxième commentaire mais je l'ai oublié.

WES HARDAKER : Beaucoup de technologies sont associées à des coûts. Donc, les FSI et tout le monde doivent faire ce qu'ils doivent faire, en ayant pleinement conscience des coûts qui y sont associés.

Ensuite, il y a aussi l'aspect qui n'est pas immédiatement visible, donc par rapport au RPKI et au DNSSEC, des coûts très importants sont associés.

JAD EL CHAM : Bonjour. Jad El Cham. Je suis boursier pour la première fois à l'ICANN. Je suis technicien, donc j'ai une question éminemment technique.

On a vu, au cours de ces dernières années, de plus en plus de fournisseurs offrant des services de sécurité par rapport au DNS pour relayer les requêtes de DNS. Traditionnellement, ils ont des centres de scrubbing pour identifier les requêtes du DNS et envoyer des réponses. Une solution, par exemple, c'est le VPN ouvert, ou encore les anti-virus, ou les logiciels anti-malware ou logiciels malveillants pour changer les serveurs DNS que n'importe quel PC pourrait utiliser.

Ma question est donc la suivante : ces solutions peuvent être une alternative au DNSSEC ? Parce que si vous regardez, par exemple, le VPN ouvert, il représente environ 2% des requêtes ou du trafic DNS.

Deuxième question : est-ce qu'elles s'entendent bien, ces solutions ?

IRWIN LANSING : Je dirais que oui, elles s'entendent bien parce que ces services de confiance répondent à votre requête pour s'assurer que vous obtenez la bonne réponse. Ils utilisent également d'autres outils du côté des logiciels malveillants

WES HARDAKER : Quelqu'un d'autre ? Merci. Excusez-moi, je ne suis pas la liste d'intervenants.

RACHEL POLLACK : Bonjour. Rachel Pollack. Je suis ambassadrice NextGen. Je travaille à l'UNESCO sur la liberté d'expression. J'ai donc une question en tant que non technicienne.

Aujourd'hui, c'est la journée internationale de la sécurité cybernétique et parfois, la censure peut s'appliquer sous cette forme.

Je me demande si le DNSSEC peut jouer un rôle pour faire en sorte que les utilisateurs puissent intervenir à ce niveau-là. Y-a-t-il une résistance politique ou autre dans ce domaine ?

WARREN KUMARI : J'ai deux réponses, ici. Oui, le DNSSEC peut au moins aider à éviter qu'il y ait censure du DNS, ou prévenir cela. Vous pouvez essayer de réduire cette exposition.

Mais comme vous le dites, il y a beaucoup de censure par rapport au DNS. De nombreux FSI ou pays surveillent les requêtes et les stoppent, cette menace est donc prise très au sérieux.

Il existe un groupe de travail appelé Deprive qui essaie de prévenir les tentatives de censure du DNS pour les requêtes envoyées aux serveurs récursifs et que vous puissiez voir si on essaie d'éviter que vous accédiez à quelque chose à quoi on ne veut pas vous laisser accéder. On travaille sur ces questions de données sensibles et de censure.

MATT LARSON : Dans la plupart des cas, s'il y a censure, c'est là que la validation DNSSEC a lieu. Par exemple, mon portable est configuré pour utiliser un serveur récursif quelque part et c'est là qu'a lieu la validation du contenu. Nous, on a conçu le protocole DNS de sorte que mon portable puisse faire une validation DNSSEC lui-même et ne fasse pas confiance à ce qu'on appelle le « last mile ».

Donc, vous faites confiance à ce que vous dit votre serveur récursif et, pour plusieurs raisons, par exemple si le serveur est très ancien ou autre, l'utilisateur final peut utiliser les différents outils à sa disposition et c'est pour ça que Warren en a parlé.

WES HARDAKER : Je crois que beaucoup des exemples qui ont été utilisés par le passé ne sont plus valables, parce que les portables ne marchent plus de la même façon.

Merci. Oui, allez-y, vous avez une question, monsieur.

SHOA ABODI : Oui. Bonjour. Shoa Abodi, je travaille pour une entreprise en Inde et sur le Forum de la Gouvernance de l'Internet en Inde.

L'une de mes fonctions est de conseiller le gouvernement de l'Inde sur l'une des propositions de la Société de l'Information qui a proposé de créer une école d'excellence sur la gouvernance de l'Internet en Inde. Que pensez-vous de la création de ce centre en Inde ?

J'ai lu une étude publiée par l'ISOC sur le DNSSEC et j'aimerais savoir, parce que j'ai développé tout un processus dans le cadre des conseils que je donne au gouvernement indien, et il y a beaucoup de problèmes sur l'amélioration du réseau pour la mise en œuvre et le déploiement du DNSSEC.

Deuxième étape, on va commencer un programme de certification et de formation pour les FSI et le rendre obligatoire pour les sites Web du gouvernement, comme NSI.GOV.IN.

Également faire en sorte que le développement du DNSSEC soit obligatoire pour les sites gouvernementaux. Donc j'aimerais savoir dans quelle mesure l'ICANN peut jouer un rôle dans cette mesure, sous forme de soutien technique.

WES HARDAKER : Jacques, vous vouliez parler ?

JACQUES LATOUR : Vous parlez de la création d'un centre d'excellente en Inde. La réponse est oui, faites-le, parce qu'il y a beaucoup d'innovations autour du DNSSEC qui vont au-delà des requêtes DNS elles-mêmes. Si vous allez à notre atelier de mercredi sur le DNSSEC, vous verrez que le DNSSEC permet l'encryptage des mails et toute une série de choses pouvant changer l'Internet.

Je pense que l'ICANN a les ressources nécessaires pour aider à la formation.

SHOA ABODI : Avec l'ICANN, nous avons organisé un atelier à Bombay. On a invité tous les fournisseurs de services Internet à cet atelier mais les gens ne sont pas en train de mettre en œuvre le DNSSEC. Ça, c'est le problème. Donc, on prévoit d'abord de faire en sorte que le DNSSEC soit obligatoire pour les sites Web du gouvernement,

puis on s'assurera que c'est un exemple. Mais avant ça, on aimerait obtenir un soutien et une formation technique de la part de l'ICANN et j'aimerais savoir qui je dois contacter pour cela. Comment l'ICANN pourrait développer, conjointement avec nous, un centre DNSSEC d'excellence, dans mon pays ?

MATT LARSON : J'y suis favorable, je crois que c'est une excellente idée. Certains de mes collègues au bureau CTO de l'ICANN font un travail de plaidoyer et de sensibilisation au DNSSEC.

Je ne sais pas dans quelle mesure on pourrait vous aider, en termes de personnel de formation, mais je vais vous mettre en contact avec mon collègue [Rick Lamb], qui n'est pas ici, mais je vous donnerai son nom. Il a énormément travaillé pour le déploiement du DNSSEC dans le monde, c'est l'une de ses fonctions. C'est la première chose qui me vient à l'esprit pour répondre à votre question.

J'aimerais aussi vous dire de venir aux réunions de l'ICANN, parce que c'est justement lors de ces réunions, lors de l'atelier de mercredi sur le DNSSEC, c'est justement à cette occasion que vous pourrez rencontrer les collègues actifs dans ce domaine. Ce n'est pas une aide de l'ICANN en tant qu'organisation, mais c'est le genre de choses qui peuvent vous aider.

WARREN KUMARI : Lorsque vous dites que les gens ne sont pas en train de déployer le DNSSEC. En fait, en Inde, il y a un déploiement plus élevé que la moyenne du DNSSEC.

SHOA ABODI : On a 400 millions d'utilisateurs Internet en Inde donc si vous comparez ce chiffre au déploiement DNSSEC, c'est un chiffre limité.

WARREN KUMARI : Même en termes de pourcentage, il y a plus de gens qui valident, je parle de pourcentage.

En ce qui concerne la signature DNSSEC des sites gouvernementaux, au début, il y a eu un certain enthousiasme, le gouvernement des États-Unis ayant dit que tous les domaines .GOV devaient être signés, ce qui a permis de faire beaucoup de progrès pour faire avancer le DNSSEC.

Ensuite, il y a des gens qui sont allés un peu réparer les problèmes existants.

WES HARDAKER : Cet effort au niveau du gouvernement des États-Unis désormais utilisés par d'autres, parce qu'en fait, ils ont été parmi les premiers à adopter le système.

D'autres questions ?

ABDERRAHMAN AIT ALI : Bonjour. Je m'appelle Abderrahman. Je suis boursier NextGen et j'ai une question assez rapide par rapport aux coûts de la transition. Je serais curieux de savoir s'il est facile, ou peut-être est-ce difficile, de passer au DNSSEC ? Y-a-t-il suffisamment de motivations pour ceux qui sont responsables de la transition, pour les convaincre, en fait ?

CHRISTIAN HESSELMAN : Pour ce qui est des bureaux d'enregistrement aux Payx-Bas, on a un programme d'incitation où, en fait, nous donnons une réduction pour le DNSSEC. Même chose en Suède. Pour tous ceux qui enregistrent un nom de domaine avec nous, donc. Le seuil est un peu inférieur pour commencer à signer des noms de domaine.

De l'autre côté, pour les FSI, pour eux, en tout cas chez moi, ce n'est pas nécessairement le coût qui les effraie, mais les appels de soutien, étant donné les erreurs de validation, par exemple. Donc, ils ont peur du nombre d'appels qu'ils vont recevoir. Ils

ont un peu peur de ça, mais les grands FSI aux Pays-Bas ont décidé de passer au DNSSEC quand même.

Dans ce cas, c'est aussi dû à un manque de compréhension de la technologie, donc ce n'est pas nécessairement le coût mais le reste.

Pour les bureaux d'enregistrement, en tout cas au Pays-Bas, ce sont des entreprises plus petites, c'est le coût de mise en œuvre. Donc il y a deux types de coût.

ABDERRAHMAN AIT ALI : Oui, mais on peut tout réduire à l'argent ? Parce que le temps, c'est de l'argent, les compétences aussi.

CHRISTIAN HESSELMAN : Oui. Pour les bureaux d'enregistrement, on utilise un programme d'incitation. Nous avons une relation de client avec eux. Pour les FSI, ils signent par eux-mêmes, en fait, ils décident par eux-mêmes de valider ou non.

Est-ce que ça répond à votre question ?

ABDERRAHMAN AIT ALI : Oui, merci beaucoup.

WES HARDAKER : Il nous reste encore un peu de temps pour une autre question. Une ou deux, peut-être.

Allez-y.

CHAWANA HUANGSUNTORNCHAI : Bonjour. Excusez-moi, une petite question. Je m'appelle Chawana et je fais partie du programme NextGen.

Serait-il possible, ou cela s'est-il déjà produit, qu'il y ait vérification par le DNSSEC, qu'on ait la case verte cochée, et que, malgré tout, ce soit un faux ?

WARREN KUMARI : Que je sache, il n'y a pas eu de problèmes techniques du DNSSEC. Il n'y pas eu de cas où le DNSSEC montrerait une case cochée qui ne le soit pas vraiment. Maintenant, que veut-elle dire ? Simplement que les données sorties du DNS sont celles qui y avaient été mises.

Donc, si quelqu'un tape la mauvaise adresse IP lorsqu'il configure son serveur de DNS, alors le DNSSEC vous montrera quand même la cache verte cochée, même si les informations mises dans le DNS étaient fausses. C'est simplement la vérification des informations incluses.

C'est bien ça, si les informations sont mauvaises, elles sont mauvaises, mais ça ne veut pas dire que le DNSSEC dit que les informations sont invalides.

WES HARDAKER : J'ai parlé à de nombreux responsables de navigateurs. Ils essaient de clarifier leur interface, de s'assurer que le vert et le rouge correspondent réellement aux informations exactes, donc c'est un peu la discussion qu'ils ont. Je crois que la réponse est complexe.

JULIE HEDLUND : Nous avons une question sur le chat d'Alexandrine Gauvin : « Comment puis-je vérifier que mon FSI a la signature DNSSEC ? »

WES HARDAKER : Excellente question. Warren, vous voulez répondre ?

WARREN KUMARI : Il me semble qu'il y a un nom permettant de se rendre sur une page, je crois que c'est comme ça que l'on fait la validation DNSSEC, pour voir si c'est signé DNSSEC.

WES HARDAKER : Il y a certains domaines qui vous indiquent si vous avez un FSI qui utilise la validation. Malheureusement, je ne m'en souviens plus. Je crois que c'est DNSSEC-ready, en anglais. On va regarder.

Donc DNSSEC-deployment.org, c'est la case cochée. Il y a autre chose également, il y a le pouce qui remplit toute la page, c'est assez évident.

CHRISTIAN HESSELMAN : Pour le .NL, nous avons un site Web où nous montrons le pourcentage de trafic que nous recevons qui exécute le DNSSEC. Ce que cela suggère, c'est l'origine du trafic, donc l'origine du trafic activé DNSSEC, avec validation donc. On lit ceci au nom des FSI, donc si vous regardez sur notre site, vous pouvez savoir quels sont les FSI qui ont besoin de signatures dans le DNSSEC, qui les demandent.

WES HARDAKER : Il y a également un marché existant qui fait des tests du résolveur de votre FSI, pas uniquement la case cochée DNSEEC, mais aussi tout un tas de points rouges et verts. C'est vraiment pour les experts, mais si vous ne voyez que des points verts, de toute façon, c'est bon.

Je ne sais pas si on a pu trouver la page de renseignements ?

Il en existe des pages comme ça où on peut trouver ces informations.

Je pense que nous avons encore le temps pour une autre question. Allez-y.

INTERVENANT NON-IDENTIFIÉ : Bonjour, je m'appelle [Masouala ?] et je voudrais poser une questions sur le système. En fait, quelle est l'interaction entre le DNSSEC et la sécurité de l'Internet ?

Si ce problème de sécurité du DNS est résolu, existe-t-il une théorie, une hypothèse selon laquelle les problèmes de sécurité pourraient être résolus ?

Si j'attaque le DNS, très bien, vous vous occupez de sa sécurité, donc où vais-je attaquer si je suis un pirate ? Quelle est la suite ?

CHRISTIAN HESSELMAN : Tout ce qui est dispositifs de fuite, c'est facile à pirater. C'est un gros enjeu en matière de sécurité sur l'Internet.

WES HARDAKER : Effectivement, c'est un point fondamental. L'internet a commencé tout petit, de manière non sécurisé et il a fallu ajouter ces solutions petit à petit parce qu'effectivement, il y a toujours un danger à venir.

J'aimerais maintenant remercier notre panel d'avoir aidé à répondre à vos questions. On les applaudit.

Alors, il y a d'autres ressources qu'on peut consulter. Vous verrez qu'on va parler du DNSSEC dans différentes présentations. Il y a également la journée technique, lundi, avec tout un tas d'informations techniques, et il y a toujours des présentations DNSSEC.

Ensuite, mercredi, nous avons toute la journée dédiée uniquement au DNSSEC. C'est à partir de 9 heures jusqu'à 15 :00. C'est un atelier extraordinaire. C'est pour ça, d'ailleurs, que je suis venu pour la première fois à l'ICANN.

Il y aura un quiz DNSSEC et vous verrez certaines des informations qui étaient à l'écran se retrouver dans le quiz, donc dans le test. Si vous avez été attentifs, vous pourrez répondre à toutes les questions et avoir une bonne note.

JULIE HEDLUND : Merci de nous avoir orientés vers cette séance, Wes vous a encouragés à venir et c'est très intéressant.

Je voulais également vous demander à tous de m'aider à remercier Wes, qui a organisé la séance d'aujourd'hui. Merci beaucoup, Wes.

WES HARDAKER : Vous ne m'avez pas donné l'occasion de vous remercier d'abord. Julie et Kathy s'occupent de toute cette présentation, s'occupent des t-shirts, etc. Merci beaucoup pour tout votre travail au cours des années, pour la mise en place de cette présentation.

Merci beaucoup, et je vous souhaite une excellente soirée.

[FIN DE LA TRANSCRIPTION]