HYDERABAD – DNSSEC pour tous : guide du débutant
Vendredi 4 novembre 2016 – 17h00 à 18h30 IST
ICANN57 | Hyderabad, Inde

WARREN KUMARI : On va laisser deux petites minutes encore aux derniers pour venir nous joindre dans la salle, avant de commencer cette séance.

Bien. Nous allons commencer. Bonjour à tous. Je suis Warren Kumari. Voici la séance DNSSEC pour tous. En général, c'est Dan York et d'autres personnes qui font la présentation de cette réunion. Malheureusement, ils n'ont pas pu être ici aujourd'hui. Et je n'ai pas le contrôle sur la présentation. Donc je ne sais pas qui a le contrôle sur cette présentation à l'écran.

Alors, qui a déjà participé à une réunion du DNSSEC ? Bien. Donc ça va ressembler à ce que vous avez déjà entendu. Bon. J'ai vu que beaucoup d'entre vous ont déjà écouté le petit sketch qu'on fait.

Alors les gens qui entendent parler du DNSSEC pensent que ça a été créé il y a 10-15 ans. En fait, c'est beaucoup plus ancien. Ça a été inventé du temps des hommes des cavernes.

Donc vous voyez ici à l'écran Ugwina. Elle vit dans une cave au bord du Grand Canyon. Et ça, c'est son petit ami Ug qui vit aussi dans une cave de l'autre côté du Grand Canyon. Malheureusement, le Grand Canyon est vraiment énorme et ça prend beaucoup de temps de passer d'un côté à l'autre du Grand Canyon. Alors Ugwina et Ug ne se rencontrent pas très souvent, et ils en sont bien tristes.

Et à l'occasion de l'une des rares opportunités qu'ils ont de se rencontrer, ils se réunissent autour d'un feu et ils se rendent compte qu'il y a de la fumée qui vient de ce feu. Et tout d'un coup une idée leur vient. S'ils utilisent cette fumée du feu, ils peuvent parler entre eux, plutôt que descendre la falaise, la remonter, pour aller voir l'autre.

Et ensuite, un jour, un autre homme des cavernes vient et fait la même chose. Il commence aussi à envoyer des signaux de fumée. Parce qu'Ugwina est loin, elle n'arrive pas à voir qui envoie ces signaux de fumée. Elle ne sait pas quels signaux de fumée elle doit croire. Donc elle est perturbée parce qu'elle pense que [dit Ug], et donc, elle descend de sa falaise, elle va de notre côté, elle commença crier sur Ug. Ils se disputent et finalement ils se rendent compte que c'est l'autre homme des cavernes qui envoie ces signaux de fumée.

Donc ils décident, Ugwina et Ug, d'aller voir l'un des sages du village. Et l'un de ces sages, l'homme des cavernes Diffie, pense qu'il y a une brillante idée.

Il va dans la caverne d'Ug et il prend une poignée de ce sable très spécial, parce qu'il n'existe que dans la cave d'Ug -c'est pour ça qu'il est spécial-, donc il en prend une poignée et il le jette dans le feu. Et la fumée devient bleue.

Donc maintenant, Ugwina peut rentrer chez elle et peut commencer à parler avec Ug, parce qu'elle sait que la fumée, les signaux de fumée d'Ug ne seront que bleus.

Et c'est un petit peu ce que fait le DNSSEC. Ça ajoute une fumée bleue pour que vous puissiez voir quels sont les véritables destinataires et quels sont les faux.

Je vais maintenant vous présenter Wes qui va vous faire cette présentation. Vous pouvez vous assoir ici, Wes.

WES HARDAKER : Bonsoir à tous. Alors on va faire une petite introduction du DNS et du DNSSEC, vous donner un aperçu, et puis faire un petit sketch pour que ce soit un peu plus amusant.

Alors, tout d'abord, le concept de haut niveau du DNS, la manière dont il fonctionne. C'est une arborescence. Ça va vers le bas comme les racines d'un arbre.

Donc on commence par le haut. La racine, c'est là où tout le monde va et on ne sait pas qui s'adresser, donc il faut s'adresser à la racine. Par exemple, si vous essayez de chercher le nom bigbank.com et vous ne savez pas par où commencer, on commence par la racine.

La racine vous dit, « Non. Je ne sais pas où trouver bigbank.com, mais je sais où est .com ». Donc vous suivez cet arbre vers le bas pour arriver et avoir les idées un peu plus claires.

Un résolveur, et c'est en général géré par votre fournisseur de service Internet local, c'est ce qu'il y a sur votre téléphonie mobile, votre téléphone mobile, votre ordinateur portable, etc. donc on pose la question, ou est bigbank.com ; il faut traverser toute la hiérarchie du DNS, depuis le haut jusqu'au bas, et chaque niveau faire référence au résolveur du niveau suivant.

Autre aspect important, le résolveur cache des informations pendant un certain temps. Donc si vous avez déjà posé la question, ça ira plus vite la fois suivante parce qu'on n'a pas besoin de s'adresser de nouveau à la racine pour poser une deuxième fois cette question puisque ces informations sont connues dans le cache.

Donc à l'époque où il n'y avait pas beaucoup de sécurité dans l'Internet, parce qu'il n'y avait pas beaucoup de mauvais acteurs dans l'Internet, donc il n'y avait pas de sécurité. Mais maintenant, les noms sont très facilement usurpés donc tout le monde peut usurper un nom même si vous n'êtes pas la personne attitrée. Donc il faut ajouter des modifications en termes de sécurité au DNSSEC. Mais une fois que vous avez une mauvaise réponse à votre cache, vous allez continuer à y répondre pour un moment.

Donc s'il y a une mauvaise réponse, on va continuer à alimenter cette mauvaise réponse. On va passer à un petit sketch, un petit jeu. Et je vais demander à mes acteurs principaux de bien vouloir se lever pour que vous voyiez, vous admiriez leur beau T-shirt.

Alors je vais demander à tous de mettre vos très beaux T-shirts. Alors ces micros sont différents de ceux que j'ai utilisés jusqu'à présent donc je ne sais pas les utiliser. Si vous savez comment allumer ce micro ? Oui. Je crois que celui-ci est allumé. Bien.

Alors, quel est l'ordinateur qui contrôle cette présentation à l'écran. Je n'ai toujours pas compris.

Alors, dans l'histoire que Warren vient de vous raconter, il y a Ug et Ugwina. Ugwina, c'est le résolveur. C'est celle qui pose la question ; la question où est bigbank.com. Et Ugwina est un peu

confuse parce qu'il y a deux versions différentes de réponses qu'elle reçoit en retour.

Alors on va commencer par le cas le plus simple. On a un utilisateur Joe, qui lève ici la main, qui a besoin d'aller sur le site Web de sa banque et dire, « Voilà, je vous en de retirer de l'argent, de faire des transactions, un virement. De payer des factures », bref. Il va devoir parler à son fournisseur de services Internet pour obtenir des réponses. Le voici.

Et ensuite, et Cathy va être le serveur racine et c'est elle qui va commencer tout cela. On a .com et bigbank.com qui va donner la réponse. Souvenez-vous qu'en fin de compte les ordinateurs ne parlent qu'avec des chiffres, des numéros, des adresses IP, etc.

Donc cela étant dit, je vais maintenant céder la parole aux acteurs.

INTERVENANT NON IDENTIFIÉ : Bonjour à tous. Je suis l'utilisateur Joe et aujourd'hui j'ai besoin de faire des choses sur mon site Web, sur le site Web de ma banque, et je vais aller sur le navigateur. Je cherche www.bigbank.com. Je veux aller donc, je le disais, sur bigbank.com.

INTERVENANT NON IDENTIFIÉ : Je ne sais pas où est bigbank.com. Attendez, je vais essayer de vérifier. Écoutez, l'un de mes utilisateurs veut aller sur www.bigbank.com, savez-vous où c'est ?

INTERVENANTE NON IDENTIFIÉE : Non, je ne sais pas. Mais je sais où est com ; c'est 1.1.1.1.

INTERVENANT NON IDENTIFIÉ : Hé .com, l'un de mes utilisateurs veut aller sur www.bigbank.com, où est-ce ?

INTERVENANT NON IDENTIFIÉ : Je sais où est bigbank.com ; c'est à 2.2.2.2.

INTERVENANT NON IDENTIFIÉ : Bigbank, j'aimerais savoir où se trouve www.bigbank.com.

INTERVENANT NON IDENTIFIÉ : Ah ! Écoutez, j'adore cet utilisateur. Dites-lui d'aller à 2.2.2.3.

INTERVENANT NON IDENTIFIÉ : Voici. Alors, écoutez monsieur l'utilisateur, j'ai trouvé la réponse. Vous devez aller à 2.2.2.3.

INTERVENANT NON IDENTIFIÉ : Très bien. Je vais donc sur mon navigateur et je fais ma transaction, celle que j'avais besoin de faire et tout va bien dans le meilleur des mondes.

WARREN KUMARI : Très bien. On reviendra vers vous pour un deuxième petit sketch dans une seconde.

Très bien. Donc voilà c'était facile. C'est comme ça que l'Internet devrait fonctionner. Tout le monde devrait répondre de façon correcte. Il n'y a pas de mauvais acteurs, et Joe peut faire ses transactions bancaires sans problème.

Malheureusement, comme on l'a dit tout à l'heure, n'importe qui peut usurper une réponse sur le DNS. Comme vous le voyez à droite sur l'écran, dans la case rouge, quelqu'un d'autre peut répondre à la place de bigbank.com ; quelqu'un d'autre peut répondre très facilement. Donc il faut faire très attention.

Nous allons voir maintenant une deuxième version du sketch et nous allons inclure un acteur malfaisant.

INTERVENANT NON IDENTIFIÉ : Comme tout à l'heure, je vais aller à bigbank.com. Je veux aller transférer de l'argent d'un compte bancaire à un autre compte bancaire. Voilà je voudrais aller à cette adresse.

INTERVENANT NON IDENTIFIÉ : Je ne sais pas où c'est, je vais me renseigner. Hey, Root, un de mes utilisateurs veut aller à www.bigbank.com.

INTERVENANTE NON IDENTIFIÉE : Je ne sais pas où c'est, mais je peux vous dire où c'est .com.

INTERVENANT NON IDENTIFIÉ : Hé .com, l'un de mes utilisateurs veut aller sur www.bigbank.com.

INTERVENANT NON IDENTIFIÉ : Je ne sais pas, mais je sais où bigbank.com se trouve ; c'est à 2.2.2.2.

INTERVENANT NON IDENTIFIÉ : Alors, un de mes utilisateurs veut aller à www.bigbank.com.

INTERVENANT NON IDENTIFIÉ : Ah ! Je peux vous aider [arrive le démon prend la parole]. Je peux vous aider avec ça. Tout ce que vous devez faire c'est aller à 6.6.6.6.

INTERVENANT NON IDENTIFIÉ : C'est génial. Ça m'a beaucoup aidé. Merci. 6.6.6.6, c'est là où vous devez aller, monsieur l'utilisateur.

INTERVENANT NON IDENTIFIÉ : Bon. Je vais mettre ça dans mon navigateur, je vais connecter avec ma banque. En ça n'a pas la même allure que d'habitude ! Mais bon. Mon compte a moins d'argent que d'habitude. Mais bon. Je pense que j'ai eu un problème.

WES HARDAKER : Alors très bon travail. Oui, on les applaudit.

Ne vous asseyez pas. Restez là debout. On va voir comment le DNSSEC règle le problème. Donc le DNSSEC a été inventé il y a peu de temps. C'est une extension sécurisante pour faire face à ce problème. Donc ce qu'on va vous montrer, c'est ce qui va se passer lorsque le DNSSEC rentre en jeu. Chaque information est signée d'une manière pour s'assurer que ces données n'ont pas été modifiées. Donc les acteurs vont vous montrer cela dans le prochain sketch.

INTERVENANT NON IDENTIFIÉ : Maintenant je sais, en tant qu'utilisateur, je connais la présence du DNSSEC. Donc je vais recommencer ma transaction.

Alors maintenant la racine .com du TLD bigbank. Tout le monde a signé avec le DNSSEC. Donc voilà la procédure que tout le monde doit faire pour créer la signature digitale.

Maintenant, je suis beaucoup plus confiant en faisant les transactions bancaires. Je demande encore une fois. Je veux aller à www.bigbank.com.

INTERVENANT NON IDENTIFIÉ : Oh vous aimez faire ça. Alors, Racine, un de mes utilisateurs veut aller sur www.bigbank.com.

INTERVENANTE NON IDENTIFIÉE : Je ne sais pas, mais je sais où se trouve .com ; c'est à 1.1.1.1 ; mais je dois signer. Je vais vérifier la signature avant.

INTERVENANT NON IDENTIFIÉ : Alors .com, un de mes utilisateurs veut aller sur www.bigbank.com. Est-ce que vous pouvez me dire où c'est ?

INTERVENANT NON IDENTIFIÉ : Non je ne sais pas où c'est, mais je sais où est bigbank.com, et je peux vous dire. Je sais que c'est 2.2.2.2. J'ai une signature 2, donc je sais que c'est vrai.

INTERVENANT NON IDENTIFIÉ : Bon très bien, je vais continuer. Bigbank.com, voilà un de mes utilisateurs veut aller à www.bigbank.com.

INTERVENANT NON IDENTIFIÉ : [Arrive le démon, prend le micro et dit] 6.6.6.6.

INTERVENANT NON IDENTIFIÉ : Non. Il n'y a pas de signature là-dessus. T'es qui toi ?

INTERVENANT NON IDENTIFIÉ : L'adresse est 2.2.2.3, et voilà ma signature.

INTERVENANT NON IDENTIFIÉ : Oui très bien. Hé monsieur l'utilisateur, 2.2.2.3 ; j'ai vérifié, j'ai eu les signatures, tout va très bien.

INTERVENANT NON IDENTIFIÉ : Ah ben maintenant j'ai beaucoup plus de confiance. Je peux aller à ma banque fermée transactions comme d'habitude.

WES HARDAKER : Merci beaucoup à tous, à tous nos acteurs. Merci tous nos acteurs de l'ICANN.

Donc, maintenant nous allons passer à autre chose. Nous donnerons plus de détails plus tard sur le fonctionnement du système.

Donc une chose importante à comprendre, c'est que le DNSSEC protège le DNS. Quand on pose la question au système DNS, vous allez recevoir une réponse. Mais cela ne veut pas dire que cela va protéger l'Internet en général. Il y a d'autres technologies qui protègent d'autres éléments, comme le système de routing, qui ont des technologies séparées qui sont développées, https qui protège http. Donc il y a des systèmes différents qui entrent en jeu. La solution DNSSEC est la solution pour ces réponses et cela, ça a été déployé pendant la dernière décennie. Et maintenant, je pense que 2010. 2010. 2010.

Donc beaucoup de TLD au-dessus de ça sont signés. Les .com sont signés. Donc le niveau de déploiement a vraiment augmenté.

Les clés et les signatures sont mises en place pour vérifier les informations, et vous pouvez obtenir les clés pour tout ce qui est au-dessus de la racine, en passant par– en demandant au DNS. Donc ce sont des clés qui permettent de faire des vérifications

sur la voie, si vous voulez. Vous devez donc demander au DNS pour la clé dont vous avez besoin.

La clé la plus importante, c'est la clé racine. Une fois que vous avez ça, vous avez tout ce qu'il vous faut pour finir le processus de sécurité. Tout est prêt [à qui]. On vous donne la clé de la racine. Toutes les réponses au-dessous de là vont correspondre. Donc comme dans ce cas-là pour bigbank.com et .com ; il y a une chaine de confiance entre ces différentes étapes.

Donc c'est la même chose que ce que vous avez vu, par exemple, dans notre sketch. Vous avez toutes les choses que vous pouvez vérifier. Vous pouvez voir ce qui est vrai. Vous pouvez dire, « Oui, j'ai reçu la réponse de .com ; c'était bien signé ». Et donc, vous pouvez ainsi dire– vous pouvez ainsi voir ce qui est vrai ce qui n'est pas vrai.

On a fait cela. On a fait ce sketch. Maintenant on va passer aux exemples pour voir pourquoi on a besoin du DNSSEC et vous donnez un peu des directives.

Ce que vous avez, c'est que vous n'aimeriez pas mémoriser une adresse IP pour toutes les banques, pour tous les sites Web que vous voulez. Les numéros de téléphone, déjà, c'est difficile. Combien de numéros de téléphone de vos amis vous devez mémoriser. Vous avez un téléphone, avec une banque de données pour tous les numéros de téléphone. C'est bien

compliqué de se rappeler de tous les numéros. Moi je ne connais pas tous les numéros de mes amis parce que j'utilise l'annuaire de mon téléphone. Donc le DNSSEC connecte les noms aux nombres. Donc les adresses Internet sont des nombres.

La chose qui est importante c'est que toutes les applications qui demandent– toutes les applications doivent passer par le DNSSEC de façon à ce qu'elles puissent être obtenues et qu'elles puissent être utilisées, pardon.

Alors pour pouvoir avoir la bonne adresse, pour ne pas être dirigé dans la mauvaise adresse, l'IETF qui a essayé pendant très longtemps de résoudre tous les problèmes à toutes les différentes couches de l'Internet, nous voulons, nous, voir la bonne adresse dès le départ. Cela comprend la capacité de pouvoir vous protéger afin qu'une personne malveillante ne puisse pas rentrer en jeu.

Si vous avez la mauvaise adresse, vous allez aller sur le site Web erroné, et vous allez rentrer vos données, vous identifiez, vos identifiants, et vous allez envoyer un courriel, par exemple, à une mauvaise adresse.

Il est donc très facile de trouver des outils DNS sur l'Internet, il est donc important que nous allions de l'avant dans la communauté ICANN, la communauté technologique, pour essayer d'avancer avec ces technologies.

Alors, comment est-ce que le DNSSEC peut aider ? Le DNSSEC nous assure que nous puissions nous diriger au bon endroit. À la bonne adresse. Au que nous ayons la bonne adresse pour aller au bon endroit. Et les signatures nous permettront d'éviter les mauvais acteurs.

Excusez-moi des termes techniques que j'emploie– oh non. Les mauvaises– j'ai des problèmes techniques avec l'ordinateur.

Pensons au même scénario. Et voilà donc une représentation graphique. Je veux que vous compreniez exactement ce qui se passe. C'est une séquence assez complexe. On en reparlera plus tard, mais en attendant, c'est un peu le diagramme de ce qui vient juste de se passer.

Lorsqu'une demande arrive, elle passe à travers beaucoup de serveurs. Vous voyez qu'avec toutes les flèches que vous voyez sur notre diagramme, vous voyez qu'il y a beaucoup de transactions en cours. Les gens ne se rendent pas compte quand ils tapent www.bigbank.com qu'il y a beaucoup de transactions qui se passent ; il y a beaucoup de serveurs qui sont inclus dans cette transaction. Il y a beaucoup de serveurs DNS qui sont inclus dans une page Web. À la fin, nous voulons la bonne réponse pour l'utilisateur. Nous ne voulons que la bonne réponse pour l'utilisateur.

Nous avons une page Web qui s'appelle dnssec-deployment.com ; vous pouvez utiliser les informations et vous pouvez ainsi utiliser les informations pour valider si vous avez une zone, ou si vous êtes propriétaire d'une zone, vous pouvez ainsi obtenir les informations pour pouvoir signer. Il y a des outils qui sont aussi disponibles pour que vous puissiez le faire vous-même. Il y a aussi des outils pour vous aider à déployer un résolveur qui utilise le DNSSEC.

Vous allez trouver une marque verte là-haut sur le coin à gauche qui peut vous montrer que si vous allez sur telle ou telle page Web, cette page est validée. Si vous allez sur cette même page et que vous voyez ce diamant jaune, comme vous le voyez à l'écran, vous pouvez voir que vous n'êtes pas protégés par le DNSSEC.

Le DNSSEC peut être mis en place à différentes étapes. Vous pourrez être protégés ou pas. Donc vous pouvez le faire aussi sur votre ordinateur portable. C'est un petit peu plus difficile. Moi je l'ai fait, mais je suis très technique. Cela est réservé souvent pour les ISP, les professionnels.

Voilà ainsi le diagramme– un peu un diagramme comme celui que nous avions auparavant. À la fin, comme vous voyez, que la personne malveillante est incluse dans ce diagramme. Comme vous voyez, cette personne, la personne malveillante, est très

proche d'utilisateurs. Sans le DNSSEC, vous ne pouvez pas forcément savoir si vous obtenez la bonne réponse ou la bonne information.

Donc la ligne rouge que vous voyez sur le diagramme va être beaucoup plus lente que la réponse du malveillant qui est beaucoup plus courte.

Voilà sur ce diagramme la mauvaise réponse du malveillant, de la personne malveillante, a été bloquée parce que le DNSSEC a vérifié la signature cryptographique, a vérifié la réponse, et a vu que cette réponse était mauvaise, donc n'a pas accepté et a continué à écouter pour voir ce qui suit. Et c'est ce qui se passe sur ce diagramme comme ce qui s'est passé sur notre sketch. Lorsque la bonne réponse attend l'utilisateur final.

Voilà ce qui se passe donc avec cette marque verte, cette marque de vérification si vous voulez. La personne la reçoit. L'utilisateur la reçoit, mais plus rapidement. Si vous avez un navigateur qui sait faire ça, ou que votre ISP sait faire ça pour vous, la mauvaise réponse sera ignorée.

Voilà un spoof que nous avons fait. Nous avons publié un article faux sur notre site, et nous avons utilisé ce système. Donc la première page avec la marque verte que vous voyez n'a pas la photo de Steve Crocker comme à l'écran, et celle qui n'est pas approuvée a la photo de Steve Crocker.

Vous vous rappelez avant quand je vous parlais de votre navigateur qui produisait beaucoup beaucoup beaucoup de questions ? Ce diagramme que vous voyez a été créé il y a une dizaine d'années, je pense. Chacune de ces lignes est une question ou une réponse du DNS. Juste en allant sur la page cnn.com ; c'est vraiment fou et c'est pire maintenant. J'ai fait ça il y a 10 ans, et maintenant il y a beaucoup plus de lignes sur ce diagramme.

Vous voulez vous assurer que chacune de ces lignes est protégée et que l'information va au bon endroit.

Le DNSSEC c'est une chose très complexe. Pardon, le DNS, c'est un système très complexe. Il y a énormément de questions qui sont posées et ce système ne se rend pas compte de combien de demandes passe à travers à travers ça tous les jours. Toutes les applications posent des questions. Il y a beaucoup beaucoup de questions DNS qui sont en jeu. Alors des informations de base au sujet du DNS. Cela fournit une traduction entre les noms et les adresses de réseau. Le DNS peut– vous pouvez à travers le DNS, vous pouvez demander des clés, vous pouvez poser toutes sortes de questions. Vous pouvez savoir quel est le serveur de courriel. Il y a plein de choses qui puissent être faites à travers ce système.

Et la chose importante, c'est de savoir que les données sont la chose la plus importante. Quand vous posez une question, vous voulez vous assurer que vous allez recevoir la bonne réponse.

Ce n'est pas grave combien de personnes l'ont utilisé avant vous. Et ça, c'est ça qui est bien avec le DNSSEC. Cela protège les données.

Si je pose une question à la première personne ici et que cela fait le tour et que ça va au fond de la salle, c'est comme le jeu quand on joue, quand on est enfant, quand on joue au téléphone rave où on pose une question à une personne et que l'information continue à passer d'une personne à une autre. Non. Ça ne se passe pas comme ça avec le DNSSEC. Peu importe le nombre de personnes qui ont eu affaire à l'information. C'est égal.

Ce diagramme, sur l'écran, que j'ai aussi créé il y a longtemps, montre toutes les étapes de la publication des données DNS. Par exemple, une personne dit, « Je veux créer un www », comment est-ce qu'ils le font ? Ils ajoutent ça à la zone de données, ils publient vers le serveur qui fait autorité, et la demande est envoyée, et la réponse est envoyée. Et le client reçoit la réponse. Le client envoie une demande et la demande va vers le serveur qui va autorité, et ainsi de suite. Voilà. C'est une seule transaction par rapport à toutes les lignes que vous avez vu sur le diagramme auparavant.

La mise en application du DNSSEC. Je vais passer à autre chose. J'ai rajouté d'autres choses pour vous ce soir. Je vais passer sur une ou deux de ces diapositives.

Alors, un des concepts les plus importants, c'est savoir qu'il faut protéger la zone des données. Si le DNSSEC protège vos données, c'est bien. Mais si vous mettez des mauvaises données, comment est-ce que vous allez savoir quelles sont les bonnes données et les mauvaises données. Beaucoup de gens se concentrent sur la conservation des clés privées du DNSSEC sans protéger les personnes qui rentrent les données. Il faut se rappeler qu'il faut protéger la sécurité, mais aussi protéger la zone.

Voilà le même diagramme que vous avez vu tout à l'heure, ou à peu près le même, mais cela vous montre les cases qui sont rajoutées au diagramme par le DNSSEC. Avant, nous ajoutions les données dans la zone de données, et maintenant nous savons que le serveur qui fait autorité va pouvoir signer les données. Il y a aussi le fait que le serveur résolveur qui valide connait la clé de la racine et peut comparer et peut confirmer les signatures.

Nous allons passer sur ces diapos aussi. Julie, je pense que vous avez des questions. Nous voulons passer vos questions avant de passer à la prochaine partie de la présentation. OK ?

Rick ? Bon. En attendant– le voilà. Voilà Rick qui vient en courant. Non, non. Ne vous inquiétez pas, Rick. On a encore le temps.

RICHARD LAMB : Je travaille à l'ICANN. J'étais– au début, on m'avait dit que l'on allait faire ces signatures de racine et on n'avait fait jamais fait ça avant. Et je me suis dit, comment les gens vont avoir confiance en nous. Comment est-ce qu'on peut faire pour que les gens aient confiance. Bon. Ce n'est pas toujours facile.

De toute façon, comme vous l'avez entendu durant cette présentation avec le sketch en particulier, au début, qui était très drôle, vous voyez une chose qui est très importante dans tout cela, c'est la confiance de cette clé. Ce n'est pas facile.

La confiance c'est quelque chose de difficile. Nous avons 21 personnes qui travaillent avec nous à travers le monde. 18 d'entre nous ne sont pas américains, pour que vous le sachiez, c'est important. Ils ont des clés physiques, ou des cartes, qui elles-mêmes ont des parties différentes. Et ces gens-là se rejoignent une fois par an pour une cérémonie de signature de clés.

En fait, c'est un processus commun qui est utilisé par les autorités de certificat. Quand on voit le petit verrouillage, quand

vous voyez les verrouillages sur les pages de l'Internet, c'est une chose commune. Nous avons un peu emprunté ce système si vous voulez.

Donc ça a été fait en 2010. Et ICANN était inclus. VeriSign était inclus dans le processus. Et nous avons fait cela la demande de la communauté.

Donc cette présentation, que veut-elle dire ?

Cela fait six ans maintenant et nous allons changer les clés. Nous allons créer une nouvelle clé. C'est très intéressant pour certains d'entre non. Mais si nous changeons ses clés comme l'avons dit tout à l'heure, ces clés font partie des résolveurs et de la plupart du réseau. Donc si nous changeons cela sans dire à ces parties prenantes que nous le faisons, cela va poser un problème. Cela va être un gros problème.

Donc si je fais cette présentation et si on m'a passé la parole aujourd'hui, c'est pour aider à ce qu'il y ait une prise de conscience et que tout le monde soit au courant de ce principe.

Comme je l'ai dit tout à l'heure, il y aura peut-être des termes un peu étranges que vous allez entendre, comme la cérémonie de signature de clés, et ainsi de suite. Non, à ICANN, on a essayé, on a dépensé beaucoup d'argent pour essayer de comprendre ces processus. Mais puisque nous sommes à l'ICANN, vous savez

comme c'est transparent, c'est ouvert, nous publions tout cela. Nous vous disons exactement où elle se trouve. D'ailleurs voilà, quand vous voyez sur la diapositive, voilà, il y a, à côté de l'aéroport de Los Angeles, comme vous le voyez sur l'écran, et puis ici aussi, 25–30 kilomètres de Washington D.C., pardon. Ce n'est pas un emplacement qui a été choisi pour une raison particulière. C'est un très bon centre et c'est un très bon emplacement.

Donc c'est pour vous montrer sur ses diapositives qu'il y a beaucoup de gens qui participent à ces cérémonies. Nous avons choisi le nom Kaminsky parce qu'il est là. Vous le voyez sur la photo. Ce n'est pas un ennemi Kaminsky. C'est un critique. Alors il faut accepter ses ennemis.

[L'interprète s'excuse, mais il y a des problèmes audio].

Ah je peux me mettre à crier. Alors, comme vous voyez Vint Cerf sur la photo, le père de l'Internet qui était inclus bien sûr. Dans le processus, vous avez Anne-Marie qui vient de Suède. Vous avez des gens qui viennent de toute partie du monde. Voilà. Ce sont les gens qui participent. Et je comprends que bientôt dans les mois à venir, nous allons rajouter des personnes à ce groupe. 21 personnes qui vont venir de toutes les parties du monde.

Comme vous voyez, j'ai déjà raconté cette histoire plusieurs fois. Vous voyez qu'il y a beaucoup d'hommes. Donc on me critique

un peu pour cela. Il serait donc bon d'avoir plus de femmes qui participent dans ce processus. Il faut quand même être actif dans la communauté DNS, et donc malgré tout on ne cherche pas des politiques. On ne cherche pas–

Je gaspille un peu de temps, mais bon je pensais qu'il serait important puisque que vous êtes nouveaux de parler un peu de tout ça.

Alors c'est une bonne hygiène cryptographique de changer la clé. On utilise ce qu'on appelle « RSA Key », qui va durer pendant peut-être encore 30 ans. Cela prendra quand même 30 ans pour que quelqu'un puisse donc casser ou démonter cette clé. On ne sait jamais. Malgré tout, les choses, de nouvelles choses, arrivent toujours. Il y a des découvertes qui sont faites. On ne sait jamais. Donc si on ne fait pas de changement de clés, on ne saura pas comment le faire si on doit le faire.

Donc la dernière chose qu'on peut dire, c'est qu'on avait dit qu'on le ferait. Comme vous le savez, si vous êtes allés aux réunions d'ICANN, ICANN n'a pas d'autorité mandataire. Les gens nous font confiance parce que nous faisons ce que nous disons. Nous faisons un suivi. Nous promettons de– nous avons promis de changer la clé, disons dans cinq ans, donc nous allons le faire.

Alors qui va avoir des problèmes avec tout ça. Nous aimerions que le DNSSEC soit déployé sur tout, mais ce n'est pas le cas. À peu près 15 % des utilisateurs mondiaux sont derrière un résolveur qui fait la validation du DNSSEC.

Combien d'entre vous ont déjà vu 8.8.8.8 ? C'est Google. Il y a trois gars à Manhattan qui ont décidé de créer ça. Mon Dieu. Imaginez ! C'est impressionnant. Et je suis vraiment content que Google ait fait quelque chose comme ça. Si nous faisons une erreur, il va y avoir des effets négatifs. Il faut s'assurer avec tous que tout le monde connaisse la nouvelle clé et qu'elle soit installée.

Si nous faisons une mauvaise configuration, beaucoup de choses vont être négatives. Si vous ne recevez pas de réponse quand vous cherchez quelque chose, cela va poser un problème. Les gens vont penser que le réseau est arrêté, que l'Internet est parti, qu'il a disparu. Donc cela prend du temps.

Voilà les documents que nous avons utilisés que vous pouvez consulter. Ces documents sont listés sur l'écran. Nous avons beaucoup de plans en place si quelque chose se passe mal ; je ne pense pas que ça sera le cas. Je pense que tout va bien se passer.

Ah oui, au fait, l'autre jour, voilà le 27 octobre sur la photo sur l'écran. Nous avons généré donc une nouvelle clé. C'est un

processus très lent. Nous avons généré une clé. Et voilà la photo sur laquelle j'ai eu beaucoup de critiques ; comme vous voyez sur l'écran, il y a beaucoup d'hommes dans la photo. Donc on a fait comme la dernière fois, lorsque la clé est générée, nous avons une page qui a une représentation, un hach, une représentation du public, des personnes qui étaient là. Et nous signons tous ce document.

Et vous voyez, cela s'est passé– ce sera installé à Los Angeles en février 2017. Cette cérémonie est ouverte à tous. Vous pouvez venir observer le processus, etc. Ce sera, mais des fois on fait un bon diner après la cérémonie. Vous voyez, comme à l'ICANN. À l'ICANN, on sait s'amuser.

Voilà les dates à venir, l'agenda à venir. Alors, vous pourrez voir les résultats sur l'Internet via le DNS. Le 19 septembre vous verrez donc une augmentation de taille.

Au mois d'octobre, 11 octobre, c'est le jour J. Voilà vos dates les plus importantes sur l'écran. Donc la nouvelle clé démarrera le 11 octobre. On a l'impression que c'est beaucoup de temps, mais nous devons commencer à lancer le processus. Je pense que tous les grands noms seront satisfaits, mais il y aura toujours quelqu'un qui n'aura pas fait sa mise à jour bien sûr.

Voilà. Ma diapositive préférée qui vous donne tous les détails sur le comment nous allons faire les choses, le fonctionnement des

choses. J'ai rajouté cela en référence. Ce que vous allez faire. Alors 8.8.8.8, oui Google. Quelle est la nouvelle clé ? Comment la configurer ? Ils sont intelligents donc ils savent parfaitement bien comment procéder. Et il y a ensuite des grands fournisseurs de services Internet qui vont suivre la même voie. Mais ensuite, il y a toute une série de processus automatiques qui vont utiliser des noms avec des normes très précises. Tout le monde va s'y ranger, donc tout le monde à suivre ces normes, adopter cette nouvelle clé. Il y a d'autres normes, des approches automatiques qu'on a mises en place qui vont permettre que cela ait lieu.

C'est Matt Larson à l'ICANN qui a élaboré cette présentation et c'est lui qui l'a indiquée ici à l'écran. Et que se passe-t-il si les choses ne marchent pas comme prévu ? Il y a une gestion de l'ancre de confiance.

Donc on s'attend ici à ce qu'il y ait des [test-pads]. J'ai écrit certains de ces systèmes de roulement de clé. Donc il y avait des gens qui voulaient tester leur système et je ne crois pas que l'ICANN va avoir un système qui fonctionne en temps réel. Donc les choses se déroulent beaucoup plus rapidement qu'en temps réel. Rien de très compliqué, mais si vous avez des questions n'hésitez pas à m'envoyer un e-mail.

Et on a parlé à beaucoup de fournisseurs aussi ; avec Microsoft par exemple. Donc de grands fournisseurs. Voilà. Vous avez ici notre Twitter, Facebook. Voilà si vous voulez me contacter, je crois que le mail c'est encore la meilleure solution, et si je ne vous réponds pas tout de suite, insistez. Insistez et je vous répondrais.

Donc voilà la présentation que je devais faire. N'hésitez pas à poser des questions, quelles qu'elles soient, et vous pouvez le faire en ligne aussi.

JULIE HEDLUND : Alors cette question nous vient d'Afifa Abbas de Dhaka, au Bangladesh. La question est la suivante, « Pouvez-vous expliquer d'utiliser la clé de signature de zone et la clé de signature de clé dans le DNSSEC » ?

WES HARDAKER : Merci, Rick, de cette excellente présentation. Merci beaucoup. Vraiment très intéressant. C'est une présentation supplémentaire qu'on ne fait pas d'habitude ici, mais on en est à un moment très important sur cette thématique. Donc on a voulu inclure cette présentation.

Donc là encore, on va prendre la question dans la salle. Si vous avez des questions sur le DNSSEC, sur quelque élément que ce

soit des présentations qui ont eu lieu, lever la main. On va vous apporter un micro et les membres du panel vont répondre.

WARREN KUMARII : Oui. Moi je peux commencer à répondre. Oui. Le DNSSEC a à chaque fois, à la fois, une clé de signature de clé et une clé de signature de zone donc pour signer d'autres clés.

Ensuite, il y a la zone elle-même qui signe la clé de signature de zone. Ensuite, il y a la clé de signature de clé que vous n'utilisez pas souvent, ce qui veut dire que vous pouvez la garder à l'abri, dans un endroit sécurisé, dans un endroit sûr. Et vous ne l'utilisez pas pour signer la zone. Donc il y a deux niveaux, là, de sécurité. Vous pouvez maintenir la clé de signature de clé à l'abri de la signature de clé et lorsque vous avez besoin d'une nouvelle clé–

Je ne sais pas si vous avez bien compris ce que j'ai voulu dire parce que j'ai répété, à l'envi, le mot-clé. Donc je ne sais pas si vous avez bien compris.

WES HARDAKER : Est-ce que vous pouvez nous donner une idée d'une zone qui a besoin de cette signature de clé. Est-ce que c'est quelque chose de permanent, parce que vous disiez que cette clé de signature de clé peut être maintenue à l'abri.

WARREN KUMARI : Oui, .com par exemple, on n'en a pas besoin toutes les minutes. Donc il faut que vous signiez constamment la zone commune.

Il y a quelque chose d'un peu plus pointu encore, c'est que certaines choses cryptographiques font que plus vous utilisez une clé, plus il est facile pour un attaquant d'utiliser à mauvais escient cette clé. Donc il y a de bonnes pratiques pour la clé de signature de clé, surtout si vous l'utilisez souvent. Ce qui veut dire que vous devriez changer votre clé de signature de zone relativement souvent, donc si vous avez une clé de signature de clé qui signe la clé de signature de zone, vous n'avez pas besoin de vous préoccuper tant de cette préoccupation par rapport au fait de changer la clé de signature de clé.

INTERVENANT NON IDENTIFIÉ : Oui. Il y a des raisons opérationnelles aussi qui différencient ces deux clés. Une fois que vous changez le KSK, vous devez passer à un autre niveau. Dans le cas de bigbank.com, il faut que je dise à .com qu'il y a une nouvelle clé. Donc ça implique plus de travail vis-à-vis du KSK.

WES HARDAKER : Merci. On passe à la question suivante.

[AWAL] : Bonjour. [Awal] de NextGen. Je pense qu'une grande partie du travail par rapport au déploiement du DNSSEC est surtout de nature technique et inclut ou implique surtout les opérateurs de l'Internet et les fournisseurs de services Internet. Donc si j'ai une demande qui ne passe pas par le DNSSEC ou qui n'utilise pas le DNSSEC, en tant qu'utilisateur, que puis-je faire ?

WARREN KUMARI : Merci. Ce que vous pouvez faire, et même si c'est un peu embêtant, c'est que vous pouvez faire fonctionner votre propre résolveur sur votre machine. Et ça implique beaucoup de travail et c'est difficile.

Une autre option, c'est de changer votre résolveur DNS à un autre résolveur qui fasse une validation DNS. Si votre fournisseur de services Internet ne fait pas, vous pouvez lui demander d'utiliser une validation DNS, ou le résolveur de Google par exemple, 8.8.8.8, qui lui valide le DNS. VeriSign opère aussi le 64.64.6– je ne me rappelle plus très bien du numéro. Mais il y a un certain nombre d'autres résolveurs ouverts qui l'utilisent.

WES HARDAKER : Nous avons aussi– nous sommes humains. Nous ne connaissons pas par cœur toutes les séquences de nombres.

Donc avant vous, il y avait une autre personne qui souhaitait poser une question dans la salle. Vous aviez levé la main avant, oui monsieur ?

INTERVENANT NON IDENTIFIÉ : Bonjour. [Abdel Menem Galila] de l'Égypte. Boursier pour la deuxième fois. D'abord, j'ai un commentaire, puis une question.

Moi j'utilise le DNS, donc pour moi le KSK est sûr. Et je pense que c'est inutile pour moi de faire ce roulement.

Ensuite, à chaque fois que l'ICANN fait un roulement de KSK, est-ce qu'il y a une mise à jour de l'ancre de confiance de leur côté ?

Et troisième commentaire, le DNSSEC ne garantit pas la sécurité de contact entre moi-même et mon fournisseur de services Internet. Donc est-ce que vous auriez un conseil à me donner là-dessus ?

WES HARDAKER : Cette dernière chose que vous avez mentionnée, c'est ce qu'on appelle le dernier échelon du problème. Et Warren souhaite répondre.

WARREN KUMARI : Oui. Je vais parler du dernier échelon du problème.

Si ce qui vous importe, c'est de vous assurer que personne n'intervienne dans la réponse que vous donne votre fournisseur de services Internet, il y a deux options. L'une, c'est d'installer un résolveur de validation sur votre ordinateur portable, peut-être que c'est l'option la plus simple. Il s'agit d'une application qu'on peut installer et qui va vous garantir qu'il va faire cette validation sur votre ordinateur portable.

À un certain moment, l'IETF travaille– à l'heure actuelle, pardon, l'IETF travaille sur une autre option ; crypter votre information entre votre ordinateur portable et votre fournisseur de services Internet. Et on essaie d'éviter que les attaquants puissent obtenir des informations. Le but principal c'était également de vous apporter une certaine sécurité par rapport à la protection de vos données personnelles. S'il y a des données sensibles, qu'on ne puisse pas voir où vous allez et qu'on ne puisse pas vous bloquer.

WES HARDAKER : Alors, point de précision. Par rapport à « l'encryptement ». On ne voit pas les données qui sont stockées.

NAVEEN TANDOM : Naveen, de l'Inde. Boursier de l'ICANN. J'ai un certain nombre de questions. Pourquoi avoir choisi une période de trois mois pour

le KSK ? Pourquoi une période si longue ? Est-ce qu'il y a une raison particulière à cela ?

WARREN KUMARI : Rick.

RICHARD LAMB : Oui, en fait, je ne m'en souviens plus pourquoi on a fait ça. Mais en fait, il y a deux raisons à cela. Le ZSK, à l'origine, a deux clés ; l'une plus courte que l'autre. Plus la clé est courte, plus elle peut être compromise. Donc il faut changer cette clé.

Donc la ZSK est changée quatre fois par an. À chaque cérémonie de clé, il y a une nouvelle ZSK. C'est la raison pour laquelle nous avons procédé ainsi. Si quelqu'un vous demande dans quelle mesure une clé qui fonctionne [24/24 7/7] est viable, certains d'entre vous répondront, « Oui, ça peut être valide, ça peut être valable pendant six mois ». Mais six mois, c'est un niveau anecdotique finalement.

Ça, c'est la première raison. La deuxième raison est plus politique. Parce que cette gestion de la clé racine c'est le lien entre l'ICANN et VeriSign. Donc on ne veut pas signer en une seule fois toutes ces clés. Donc il y a des motifs et des raisons politiques derrière cela. Mais la principale raison, c'est d'ordre cryptographique.

WARREN KUMARI : Dernière question.

NAVEEN TANDOM : Donc est-ce qu'on continue à suivre le 142 ?

RICHARD LAMB : Bon. Alors pour répondre à votre question, quel choix on a ? On a le niveau 5 ? 4 ? Je vais laisser Warren répondre à cela. Il y a une norme finalement qu'il faut suivre parce que l'idée c'est qu'on est des bureaucrates et qu'on veut suivre une norme de sécurité. Mais ça, ça a une raison d'être. Il y a une norme ISO là-dessus.

WARREN KUMARI : Oui. Je voulais reprendre ce que disait Rick.

C'est notre option ? À l'heure actuelle, il y a un nombre limité de personnes qui font des HSM. Et encore moins de monde qui utilise des clés cryptographiques.

Il y a un grand nombre de personnes qui ont essayé d'attaquer les HSM, et d'une manière générale avec succès. Toutefois, beaucoup des fournisseurs HSM sont basés ou l'ont été aux États-Unis ou dans d'autres pays.

Et à l'heure actuelle, il y a un projet qui est intitulé [Criptic]. Il s'agit d'un projet mondial qui essaie de faire participer le plus de gens possibles dans le monde pour mettre en place un processus HSM tout à fait ouvert pour que tout le monde puisse valider la conception, et que chacun puisse élaborer son propre HSM ; en sachant que son HSM n'est pas le même que celui de son voisin.

Donc les HSM sont des boites chères, et ça pour une raison particulière.

WES HARDAKER : Merci beaucoup ; excellente question. Question suivante.

INTERVENANT NON IDENTIFIÉ : [MAHA GULA] de l'Afghanistan. Est-ce que les résolveurs sont ouverts au monde entier ? Voilà ma question.

WES HARDAKER : Vous demandez est-ce que tous les résolveurs sont ouverts au monde entier, ou certains résolveurs ? Ça, c'est une bonne question.

Peut-être que vous avez plus d'autorité que quiconque ici dans la salle pour répondre.

WARREN KUMARI : Ça dépend du type de résolveurs auquel vous pensez. Est-ce que vous pensez aux résolveurs faisant autorité, résolveurs de racine ? Oui. Ils sont ouverts à tous.

Les résolveurs qui ont des informations et les rendent disponibles, en général, ces résolveurs-là sont ouverts à tous. La plupart des résolveurs de fournisseurs de services Internet ne sont disponibles qu'à leurs clients. Pourquoi ? Pour des raisons de sécurité. S'ils étaient disponibles et accessibles par tous, ils pourraient faire l'objet d'attaques, de menaces, parce que n'importe qui pourrait commencer à envoyer des requêtes, des demandes, etc. Donc le même genre de résolveurs qu'ont les fournisseurs de services Internet.

Et ensuite, il y a un certain nombre d'entreprises qui ont leur propre résolveur, 8.8.8.8, etc., Google et d'autres qui font en sorte que leurs résolveurs soient disponibles dans le monde entier, et essaient d'atténuer les risques d'attaques.

WES HARDAKER : Oui. J'aimerais ajouter à cela qu'il a été dit qu'il y a trois grands résolveurs qui n'ont pas d'adresses 8.8.8, etc. ; ça ne veut pas dire que votre structure locale ou fournisseur de services Internet, gouvernements, etc., peut vous empêcher d'y accéder. Donc parfois il y a des intérêts corporatifs qu'il faut que vous ne pouvez pas y avoir accès. Donc on ne va pas rentrer dans le

détail des enjeux politiques, mais il faut bien comprendre qui fait la demande et quelles sont les raisons impliquées.

Autre question dans la salle ?

INTERVENANT NON IDENTIFIÉ : Oui. La question est la suivante. Si vous avez un co.in, et un serveur qui opère, comment est-ce que vous gérez ce KSK.

INTERVENANT NON IDENTIFIÉ : Alors vous dites, si vous avez deux niveaux de zone dans le TLD co.in, dans ce cas de figure, comment est-ce qu'opère le DNSSEC ? Comment a lieu la transition de confiance. Donc vous signez .in puis vous dites que co.in c'est une entité différente, et ensuite vous créez un lien entre les deux.

Et avec co, il y a un contenu avec les clés de co. Ça c'est une manière de procéder. Et l'autre, c'est de faire in.co avec un terminal particulier. Et tout ce qui a lieu à l'intérieur de la zone se fait avec la même clé que [.t].

Donc vous pouvez utiliser .in pour tout faire, ou co.in pour le faire.

WES HARDAKER : Ce qu'on n'a pas mentionné dans le petit sketch qu'on vous a montré, parce que c'est complexe, c'est que toutes les clés–

vous pouvez avoir 25 niveaux. Du moment que vous commencez avec la clé racine, il y a un lien sur entre chaque parent et chaque enfant. C'est-à-dire que la clé racine connait la clé et connait le lien de sécurité. Et pour .in, on dira « Voilà, j'ai des enfants, dont co , ça c'est un lien sûr ».

Donc le résolveur qui fait tous ces liens peut aller jusqu'à la fin grâce à ce lien sûr, et vous pouvez vérifier toute cette chaine tout au long de la chaine.

Alors, une question ici à l'avant.

[SARATA] : Bonjour. Sarata du Ghana, boursière. Je crois que vous avez répondu en partie à ma question.

Alors, mettons qu'il y ait une personne malveillante qui n'est pas en dehors du système. J'ai l'impression que cette personne malveillante va maintenant s'introduire dans la signature et va revenir. Est-ce qu'il y a une manière de l'éloigner totalement, une fois pour toutes ?

WARREN KUMARI : Oui. Parfois on essaie de rendre les choses plus simples en disant que le diable, la personne malveillante, appelez-la comme vous voulez, cette personne malveillante vient avec une

signature dans certains cas. Et la manière dont vous pouvez détecter que c'est un problème, c'est du fait que .com parle à bigbank.com, lui donnant une signature. Et lorsque le résolveur du fournisseur Internet demande à .com où est bigbank.com, il lui dit, « Bigbank.com se trouve là, et voilà à quoi ressemble sa signature ».

Donc une fois que le résolveur s'adresse à bigbank.com, il vérifie la signature. Et lorsque la personne malveillante apporte sa réponse, le fournisseur de services Internet connait déjà la bonne réponse et peut vérifier. Je ne sais pas si j'ai bien répondu. Si j'ai été clair. Un peu.

WES HARDAKER : Ce qu'il faut retenir, et c'est important, c'est que le DNSSEC protège le DNS. Il ne vous protège pas contre d'autres formes d'attaques qui ont lieu en dehors du DNS, comme l'ingénierie sociale par exemple. Si quelqu'un dit je suis bigbank.com, j'ai besoin de changer ma clé, ça, ça peut avoir lieu sous forme d'attaque d'ingénierie sociale. Donc il faut s'assurer qu'il y a une vérification de qui vous êtes lorsque vous appelez un bureau d'enregistrement pour dire voilà j'ai besoin de changer cette donnée. Et ça, ça doit se faire en dehors de ce à quoi sert le DNSSEC. Vous avez compris ce que je voulais dire ? Oui ?

[JEN CHANG] : [Inaudible] J'ai deux questions ; est-ce que vous voulez que les pose [une] ? Vous répondez ensuite ?

WES HARDAKER : Allez-y.

[JEN CHANG] : Alors l'idée du DNSSEC est excellente, mais il y a encore des fournisseurs de services Internet qui ne déploient pas le DNSSEC. Et pourquoi ? Pourquoi est-ce qu'ils ne le font pas ?

Deuxième question. On sait aussi que certains fournisseurs de services récursifs ne vont pas jusqu'à la racine, parce qu'ils vont jusqu'à la zone racine et ça s'est stocké au niveau local. Donc est-ce que ça, ça engage la chaine de confiance ou pas ?

WES HARDAKER : Oui. Je vais répondre à la première question. En fait, je n'aurais pas dû vous laisser poser les deux questions en même temps.

Oui. Pourquoi on ne déploie pas le DNSSEC ? Alors, certaines personnes ne le déploient pas. On se demande pourquoi. C'est pourquoi on organise ces réunions pour sensibiliser, expliquer.

Deuxièmement, il n'y a pas suffisamment de gens qui travaillent pour ces fournisseurs de services Internet. Mais la bonne

nouvelle, c'est que beaucoup de logiciels de résolveurs sont complexes.

Ensuite, les utilisateurs, lorsqu'ils appellent leurs fournisseurs de services Internet, leur disent, « Écoutez, je sais que je ne suis pas protégée. Est-ce que vous pourriez le faire ». Peut-être qu'ils auront une réponse à vous donner pourquoi est-ce qu'il ne déploie pas le DNSSEC. Je ne sais pas. Il faudra leur poser la question. Parfois ils nous répondent qu'ils n'ont pas les effectifs suffisants. Certains nous disent, « Je ne le comprends pas suffisamment bien, j'ai besoin d'apprendre davantage sur le DNSSEC avant de pouvoir le déployer ».

WARREN KUMARI : Deuxième question très intéressante. Il y a un document qui a été produit par l'IETF qui dit que les résolveurs peuvent maintenir une copie de la zone racine, et ainsi ils n'ont pas besoin à chaque fois d'aller chercher la réponse dans la racine.

Donc il y a une copie qui contient toutes les signatures pour tous les TLD. Donc lorsque le DNSSEC fonctionne, plutôt que d'aller dans la racine, il regarde à l'intérieur de lui-même. Et déjà, il a toutes les signatures nécessaires. Et tous les « hachs » ; en tout cas, toutes les informations pour les signatures. Donc il peut faire la vérification qui suit. Il ne s'agit pas simplement d'aller faire la demande à la racine.

WES HARDAKER : Oui. Toutes les informations qui sont contenues dans la racine, ça fait partie des fonctions IANA. Donc tout cela, ça a à voir avec les données. Vous pouvez voir quelles sont les modifications qui sont faites parce que la chaine du DNSSEC commence par une clé. Si vous connaissez cette clé, alors vous pouvez vérifier tout ce que disent les gens. Le DNSSEC ne protège pas les transactions entre vous et moi, mais elle peut vous garantir, cette clé, que personne n'a modifié le lien entre vous et moi.

WARREN KUMARI : Oui. Pour compléter ce que vous venez de dire, la raison pour laquelle ce document existe c'est parce qu'il y a une protection dont Wes a parlé. Le fait que le DNSSEC a toutes ces données c'est que lorsque vous avez une validation, peu importe d'où provient cette information.

WES HARDAKER : Merci. Vous avez une autre question dans la salle ?

INTERVENANT NON IDENTIFIÉ : Bonjour. [Inaudible]. J'ai une petite question liée aux résultats.

Alors vous avez parlé [d'encryption] pour la clé.

WES HARDAKER : Oui. Excellente question. Est-ce que quelqu'un a les chiffres en tête ? Rick ?

[JACK] : L'ISOC a écrit un document là-dessus il y a cinq ans, je crois. Les chiffres à l'époque tournaient autour de 10 % par rapport au DNS, mais ça, c'était il y a cinq ans. Je pense qu'aujourd'hui on en est à peu près au même niveau de résultats.

WARREN KUMARI : Malheureusement, comme pour toute question technique, ça dépend et c'est complexe. Alors lorsque vous parlez des résultats, ça dépend de ce dont vous parlez. Donc effectivement, on a besoin de plus de recherche DNS. Ça dépend du trafic DNS.

Mais je pense que votre question porte sur le CPU. Donc pour faire la validation, j'ai vu des chiffres publiés qui étaient moins de 1 % de chargement CPU. Donc c'est un chiffre vraiment négligeable. Mais il y a des caches aussi. Donc c'est encore plus minime. Donc d'une manière générale, la réponse c'est que pas suffisamment.

WES HARDAKER : Merci. [Julie].

NASRAT KHALID : Bonjour. Nasrat d'Afghanistan dans la salle. J'ai une question sur les DNS publics. Pourquoi est-ce que c'est gratuit et pourquoi est-ce que Google nous rend ce service ?

Question suivante qui porte sur les complications. Lorsque vous utilisez ce DNS public, alors vous avez des complications dans votre réseau. Je l'ai vu à plusieurs reprises. Et combien de temps ça prend en plus par rapport aux résolveurs habituels ?

WARREN KUMARI : Je peux probablement répondre à ces deux questions de la même manière. La raison pour laquelle Google fournit cela, c'est parce que la latence lente à une implication là-dedans. Beaucoup de fournisseurs de services Internet ont des résolveurs très lents ; la raison c'est parce que Google aimerait– la raison pour laquelle Google a proposé cela, c'est parce qu'ils veulent obtenir des gains et donc faire de l'argent avec cela. Donc Google rend l'Internet plus rapide pour les utilisateurs, s'assure que les utilisateurs obtiennent la bonne information.

Il y a un certain nombre d'années, un certain nombre d'entreprises fournissaient de mauvaises réponses. Si vous introduisiez un nom erroné, vous obteniez une réponse erronée. Aujourd'hui, Google veille à ce que vous obteniez la bonne

réponse. Donc la latence devrait être meilleure que celle que vous offre votre fournisseur de services Internet.

Alors, si vous trouvez que les choses ne s'arrangent pas avec le DNS public de Google, alors ne l'utilisez pas. Est-ce que j'ai répondu à votre question ?

WES HARDAKER : Oui. Je pense que c'était une bonne réponse. Vous êtes d'accord ?

INTERVENANT NON IDENTIFIÉ : [L'interprète s'excuse, mais l'intervenant n'a pas de micro].

WES HARDAKER : La personne parle des données et se demande si Google utilise les données.

WARREN KUMARI : Oui. Les politiques de vie privée de Google sont publiées sur l'Internet. Ils fournissent les informations sur les données qu'ils utilisent, et toutes les informations sont publiées sur google.com/developers/public. Si vous cherchez « Google DNS privacy », vous allez trouver toutes ces informations. Et je peux

vous dire que toutes ces informations sont vraies. Mais personnellement, je peux vous dire que c'est ce que l'on fait, on vérifie, et j'en suis témoin. Ce sont des informations vraies.

[BETTINA] : [Bettina] de Thaïlande. Boursière. Il y a quelques années, j'ai essayé de participer au lancement du DNSSEC en Thaïlande. La chose difficile pour moi, c'était de parler de budget parce que c'était un sujet très compliqué. Les gens ne comprenaient pas. C'était technique. Alors ils se disaient, « Ah oui, puisque c'est compliqué, les pirates vont trouver ça compliqué aussi ».

Comment est-ce qu'on peut justifier comment cette situation est compliquée et difficile. Est-ce que vous avez fait des recherches, ou est-ce que vous avez des informations qui pourraient nous aider ?

WES HARDAKER : Oui. C'est une bonne question. Ça va m'aider à répondre à la question préalable. Pourquoi est-ce que les gens n'utilisent pas de validateur aujourd'hui ?

Il s'agit bien sûr de budget. Cela coute de l'argent. C'est comme toutes les choses nouvelles qu'on utilise.

RICHARD LAMB : Oui. Moi j'ai la religion DNSSEC. Oui, pour beaucoup d'entre nous, il ne s'agirait pas de protéger le DNS. Il s'agit de penser à un système dans lequel on pourrait échanger des informations clés entre tout le monde. Disons que je veux vous envoyer un message crypté, je peux le faire. J'utilise le DNS. Je recherche la clé. Je fais un message crypté. Je l'envoie à votre ordinateur. Vous pouvez vérifier ma clé. Vous avez la copie de la clé. Vous pouvez décrypter. Donc ainsi, toute l'information devient une base de données protégée mondiale, que tout le monde peut utiliser pour échanger des informations.

Nous savions déjà cela avant, mais en 2010, on s'est rendu compte qu'il se passait beaucoup plus de choses. Donc cela est ma réponse.

Et d'autre part, 90 % des TLD ont déployé le [TLD] ; au deuxième niveau, nous n'en sommes qu'à 2 % ou 3 %. Donc pour nous, nous savons qu'il y a là une opportunité.

Je sais. Ça a l'air d'être– j'essaie de faire des ventes. Mais bon. C'est comme ça.

WES HARDAKER : Vous pouvez utiliser par exemple Google pour avoir des informations sur le piratage de DNS. Je n'ai pas l'information là, comme ça, pour vous, mais il y a un catalogue entier là-dessus.

Il y a eu beaucoup d'articles qui ont été publiés sur le piratage du DNS, sur l'empoisonnement des caches, etc., etc.

Donc ça, c'est une information que vous pouvez aller consulter, et ainsi vous pouvez voir qu'il y a eu beaucoup de choses comme ça qui se sont passées par le passé. Est-ce que nous avons une protection totale maintenant ? Non. Nous pouvons revenir en arrière et dire que pour protéger tout, il faudrait qu'on protège tout à toutes les étapes, toutes les couches de l'Internet. Et l'IETF, ils travaillent d'ailleurs.

INTERVENANT NON IDENTIFIÉ : Le DNSSEC, c'est une plateforme pour l'innovation. Il s'agit de l'Internet des choses qui connecte tout. L'Internet des choses a besoin d'énormément de sécurité, et ça, c'est le DNSSEC. Et c'est important à l'infrastructure, si vous voulez. C'est comme ça que vous pouvez le vendre.

WES HARDAKER : Est-ce qu'il y a quelqu'un qui veut poser une question dans la salle ?

[GIGI] : Je viens des États-Unis et je me demande si vous pouvez nous donner des informations sur la mise en application du DNSSEC de la part des nouveaux gTLD.

WES HARDAKER : Quelqu'un veut parler du modèle des nouveaux gTLD ?

RICHARD LAMB : Je ne travaille pas vraiment avec les nouveaux gTLD, mais bon je peux vous dire qu'il est requis pour les nouveaux gTLD de déployer le DNSSEC. Les fournisseurs de backend, comme je l'ai déjà dit, savent que les nouveaux gTLD ont des gens qui gèrent leur infrastructure pour eux. Ils sont tous très au courant du DNSSEC.

Comment est-ce qu'ils le mettent en application ? Je ne sais pas. Moi je donne un cours. J'ai un cours de quatre ou cinq jours, que je fais. Je vais à travers le monde pour donner ce cours, cette classe. Je ne l'ai pas encore fait aux États-Unis, mais je veux venir pour vous expliquer comment tout cela fonctionne ; la cérémonie des clés, la signature des clés, ainsi de suite [inaudible].

Vous ne pouvez pas utiliser les fournisseurs qui sont déjà sur place. Il y a des solutions commerciales qui fonctionnent bien. Moi, je pense comme le DNSSEC doit– demande une certaine

compréhension, il n'est pas facile de le faire soi-même. Il faut vraiment savoir que si quelque chose se passe mal, il faut pouvoir le comprendre.

WES HARDAKER : Nous n'avons presque plus de temps, mais nous pouvons prendre une question de plus.

[AWAL] : Je pense que, par exemple, si j'essaie de résoudre un domaine et si quelqu'un, une personne malveillante, essaie de faire quelque chose de mal, et que le DNSSEC fonctionne, en tant qu'utilisateur, est-ce que je peux obtenir des informations pour savoir si la chaine de confiance a été cassée, disons ? Ou est-ce que comment je vais obtenir un avis ? Ou comment est-ce que je fais pour savoir ?

WARREN KUMARI : Oui. En tant qu'utilisateur de tous les jours, il est bien difficile de savoir exactement comment les choses se sont passées, si vous voulez, parce que le résolveur va ignorer la réponse. Le résolveur ne va pas vous dire que quelqu'un essaye de vous mentir. Si vous avez votre propre résolveur, peut-être pouvez-vous alors regarder dans les dossiers pour savoir s'il y a un paquet erroné qui a été reçu. Donc à la base, vous ne devriez jamais voir quelle

est la mauvaise réponse de votre attaquant parce que cela n'a fait aucune différence pour vous.

Je pense que c'est ça la réponse.

WES HARDAKER : Oui. Moi j'ai déjà travaillé sur des dossiers comme ceux-là, et je peux vous dire que vous pouvez avoir l'information sur certains résolveurs. Mais il faut vraiment avoir ce logiciel sur votre ordinateur pour pouvoir savoir.

Une autre question et ensuite on va devoir fermer– terminer cette réunion. Prenez le micro s'il vous plait.

INTERVENANTE NON IDENTIFIÉE : Oui. Vous avez posé la question de l'utilisateur final. Et ma question a donc à voir avec est-ce qu'il pourrait y avoir un plug-in pour un navigateur ? Est-ce qu'on pourrait installer cela ? Et, quel que soit le navigateur qu'on utilise, on pourrait avoir une alerte, si vous voulez ?

WES HARDAKER : Puisque j'ai écrit moi-même un plug-in qui fait cela, je peux vous dire que je sais que si vous allez sur Firefox ou sur Chrome, il y a quelque chose qui va attraper, disons, tout cela. Il n'y a pas quelque chose de spécifique. Il y a beaucoup de choses

techniques à faire. Mais nous, du moins la compagnie pour laquelle je travaillais auparavant, nous avons travaillé sur un système qui fonctionne avec Firefox. Et c'est quelque chose que vous pouvez faire à votre niveau, le niveau de l'utilisateur final, de la même manière que votre ISP vous aide avec beaucoup d'autres choses, sur comment faire le routing, comment envoyer les paquets au bon endroit.

Et en général, l'utilisateur final n'a pas besoin de savoir que l'ISP l'a déjà protégé. L'ISP se préoccupe des pare-feux, se préoccupe du routing, se préoccupe de la gestion de toutes les boites. Il y a tellement de choses que l'utilisateur final n'a pas besoin de savoir vraiment.

Donc je peux vous dire que si les informations malveillantes sont arrivées vers vous, vous n'avez pas besoin de le savoir.

JULIE HEDLUND : Encore une question. Vous avez une question à distance. Il y a une question à distance. « Est-ce que les nouveaux TLD ont mis en application DANE » ?

WES HARDAKER : Les TLD, en général, n'ont pas besoin de DANE. DANE c'est une technologie dont nous n'avons pas parlé ici [inaudible] qui attache un certificat au DNS pour pouvoir vérifier cela. Les TLD

ne le font pas. Les TLD n'ont pas de certificat, mais les utilisateurs en ont.

Il y a– si vous cherchez DANE ou SMTP, vous verrez qu'il y a un catalogue de toutes les données. Je pense qu'il y a 3000 et quelques domaines qui les utilisaient. Beaucoup d'entre eux venaient des ISP en Allemagne.

WARREN KUMARI : Rick disait que le DNSSEC protégeait le DNS, mais crée aussi une plateforme pour faire d'autres choses. DANE fait cela.

Vous savez, maintenant, c'est beaucoup utilisé pour le courriel. [Ness] d'ailleurs aux États-Unis déjà a publié un document là-dessus, et l'organisation [ALD] en Allemagne pour la sécurité de l'information a, elle aussi, publié un document là-dessus.

WES HARDAKER : Merci beaucoup. Merci au panel pour toute sa collaboration.

Si vous avez d'autres questions, rappelez-vous que le site de déploiement du DNSSEC a beaucoup de réponses à vos questions.

JULIE HEDLUND : Merci à Wes. Merci à Wes, l'unique Wes.

[FIN DE LA TRANSCRIPTION]