BUENOS AIRES – DNSSEC pour débutants
Lundi, Novembre 18, 2013 – 17:00 à 18:30
ICANN – Buenos Aires, Argentine

JULIE HEDLUND: Soyez les bienvenus à cette réunion DNSSEC pour tout le monde, je vous invite à venir nous rejoindre ici à la table en U pour participer à cette merveilleuse activité d'aujourd'hui et croyez-moi ça va être très intéressant et n'hésitez pas à venir ici à l'avant autour de cette table et j'essaie de régler le problème avec la caméra, mais ce que l'on va percer commencer avec la première partie et je vais résoudre ce problème de diapos mais on va commencer.

PRESENTER: Bonjour à tous, on va commencer et on va finir avec la caméra c'est ce que nous aimerions faire mais nous avons un problème technique et c'est ce que nous sommes en train de résoudre. Donc ce problème de caméras n'a rien à voir avec le DNSSEC, donc vous êtes ici à la réunion du DNSSEC manuel pour débutants, c'est intitulé peut-être intimidant et ses complexés mais c'était unique et il y a beaucoup de jargon et donc on ne va pas vous faire de vous un expert de DNSSEC mais on va vous donner une introduction générale du DNSSEC pour que vous ayez une idée de jargon et que vous ne soyez pas surpris mais avant de commencer j'aimerais vous présenter certaines desserve un intervenant qui sont à côté de moi, il y a Russ Mundy qui vient des experts scientifiques des réseaux, il a participé à nos travaux depuis longtemps, à côté de lui Roy Arens, et les chercheurs à Nominet pour le registre.uk,

il a créé beaucoup de petits DNS, à côté de lui Julie, on me demande de parler plus fort ça va mieux quand ça vous pouvait m'entendre? Julie et nous aident à organiser tout cela, à côté xxx directeur des services DNS, il me manque Jacques qui travaille pour SIRA et le registre.ca et à côté normalement il y a xxx mais on ne sait pas où il est. Donc combien de personnes issues présentes dansent la salle au sujet du DNS? Alors qu'il lançait un peu plus sur le DNSSEC?

Malheureusement je dois vous dire que tout ce que vous avez sur l'histoire de DNSSEC est probablement faux, vous pensez que ça avait été inventée il y a 10 ou 15 ans mais en fait ça était inventée il y a près de 7000 ans. Xxx qui a été une femme historique, vous voyez un autre inventeur xxx qui vivait de l'autre côté du grand canyon et ils avaient quelque chose entre eux, il y a beaucoup d'espace autour du grand canyon et il ne se voyait pas aussi souvent qu'il le souhaitait, mais lors de leur rare rencontre ils se sont regardés dans les yeux et ils ont vu quelque chose qui se sortait de ce feu, ils se sont rendus comptes qu'ils pouvaient utiliser le feu pour communiquer entre. Dont ils s'envoyer des messages, et puis un jour xxx pense que c'est intéressant d'envoyer des messages aléatoires entre leurs messages, dont il va dire à xxx à quel point il aime et il envoie des messages aléatoires à propos des bananes par exemple mais xxx ne comprend rien, elle ne sait plus quel est le vrai message et quels sont les messages inventés envoyés par xxx. Donc elle s'énerve, elle traverse le grand canyon après une traversée de trois jours, elle remonte le chemin est ils essaient de voir ce qu'ils peuvent faire pour résoudre cette situation. Dont ils vont voir les anciens et voir ce qu'ils peuvent faire pour voir comment ils peuvent parler entre eux sans que xxx ne s'en mêle, et l'un d'entre eux dits que il

va analyser le travail et tout d'un coup il a une idée merveilleuse, il se lève et il rentre dans la grotte et enfant de cette grotte il y a un message spécial ce qui fait qu'il est spécial ce que on ne trouve que dans cette grotte, dont il ressort de cette grotte est il allume un feu qui prend une couleur bleue. Maintenant ils peuvent poursuivre leurs conversations en toute tranquillité parce que maintenant elle doit écouter les messages uniquement qui sont les messages en bleu, donc chaque fois qu'elle recevra d'autres messages elle ne va pas les prendre en considération. Donc si vous devez retenir quelque chose de cela c'est que le secteur de DNSSEC envoie des messages bleus, il nous donne l'opportunité pour les destinataires de savoir que le message est sure et qui permet donc aux destinataires de savoir qu'il s'agit du bon message.

ROY ARENS: Bonjour à tous, je vais vous parler du DNS et du DNSSEC, tout d'abord j'aimerais vous poser une question, je sais que on l'a fait auparavant mais cette fois-ci c'est d'une autre manière. Tu sais que nous avons des serveurs racines dans le monde? Qui a des notions de base du fonctionnement du DNS? Alors la première diapo s'il vous plaît, voilà donc xxx et puis le deuxième domaine xxx etc. dont on sait qu'elles sont les serveurs de racines. Joe je vais vous en parler après, il n'a aucune idée du DNS, il ne peut pas parler du ISP, donc l'ISP doit parcourir tout ce chemin et obtenir l'adresse est cette information et stockée pour une utilisation ultérieure. Donc à ce moment précis gêneraient vous montrer comment on fait le DNS, voilà les principaux éléments. Alors ma diapo précédente vous montrait le serveur racines etc. alors je laisse le soin à mon équipe de régler le problème technique et xxx va jouer le rôle des

utilisateurs, xxx qui essaie de naviguer et qui tape une adresse et tout ce qui va vous montrer ici c'est ce qui ils se produiront général une fois que vous avez tapée enter et avant que la page n'apparaisse. Donc c'est une très courte période de temps et soyez assurés que même les problèmes techniques nous arrivent à nous parce que nos moments savoir beaucoup plus vite. Donc nous avons l'utilisateur Joe qui se trouve ici et nous avons notre fournisseur de l'Internet ici et le service de racines ici, et voilà le Bigbrand de com, et donc je vais passer le micro à xxx.

JOE USER: Bien, donc je suis l'utilisateur Joe qui a réglé ces factures et qui veut naviguer un peu, je ne sais pas combien je dois régler pour les fournisseurs de services Internet ISP, mais il s'agit justement de payer ma facture. Donc je m'assois devant mon ordinateur et je tape www.bigbank.com.

ISP: Merci l'utilisateur Joe, je suis un fournisseur de services Internet est la seule chose que je sais c'est où se trouve la Racing, Programmé pour cela uniquement et donc je vais demander à la racine savez-vous où se trouve bigbank.com?

ROOT: Non excusez moi je ne sais pas où ils se trouvent, mais je sais où se trouve.COM mais vous devrez poser la question à mon voisin.

ISP: Merci beaucoup, Hey.com je suis à la recherche de bigbank.com, savez-vous où je peux le trouver?

COM: Non, je ne sais pas où se trouve www.bigbank.com, mais je sais où se trouve 2.2.2.2.

ISP: Merci, écouter jusqu'à cette adresse ne savez-vous où je peux la trouver?

BIGBANK: Eh bien effectivement je sais au cette adresse se trouve, il se trouve à 2.2.2.3.

ISP: Merci beaucoup, Joe l'adresse est 2.2.2.3 bigbank.com.

JOE USER: Voilà donc l'adresse pour ma banque, est la suivante et je peux maintenant procéder au paiement. Donc la transaction est un peu plus rapide que cela, mais c'est un petit peu comme cela que ça fonctionne. Ce que l'on va faire maintenant c'est vous montrer la chose suivante, c'est une motivation un petit peu derrière le DNSSEC, et envoie faire la même chose. Je reprends mon exemple je tape mon adresse www.bigbank.com.

ISP: Merci Joe, vous voulez aller à Bigbank? Attendez je vais demander aux routeurs est-ce que vous savez où ça se trouve?

ROOT: Non, excusez-moi monsieur le fournisseur d'Internet je ne sais pas où ça se trouve, tout ce que je sais c'est où se trouve.com et c'est 1.1.1.1.

ISP: Bonjour je cherchewww.bigbank.com?

COM: Je ne sais pas où cette adresse se trouve, mais je sais où se trouve Bigbank.com, c'est adresse 2.2.2.2.

ISP: Merci beaucoup, bonjour Bigbank je cherche www.bigbank.com. Avez-vous l'adresse IP?

DR. EVIL: Oui je l'ai, l'adresse est 6.6.6.6.

ISP: Merci beaucoup, Joe voilà l'adresse 6.6.6.6. Vous devez vous connecter ici pour faire tous vos transactions en ligne.

JOE USER: Merci, donc je crois que je suis en train de me rendre sur bigbank.com, mais chacun a sa propre adresse et donc ma banque doit s'adresser à toutes ces personnes-là pour trouver l'adresse. Ce que on l'a voulait vous montrer que c'est tout ce que fait le DNS pour le DNSSEC et comment cela fonctionne dans les grandes entités, et cela fait parti des différentes connaissances dans la hiérarchie qui ne partage pas leurs informations et qui ne se connaissent même pas. Donc on revient à l'exemple de la fumée bleue, il y a une chaîne de confiance ici qu'ici que le serveur partage des clés, et c'est la fumée bleue qu'il va partager alors il faut une chaîne de confiance.

ROY ARENS: Avant de passer au prochain exemple il faut que je vous précise quelque chose. Vous vous souvenez de la diapo où nous avons Ogwina à gauche, donc Ogwina elle est celle qui reçoit, c'est une femme moderne qui est en conversation avec plusieurs serveurs, et comme vous le savez elle ne sait pas quel est le véritable serveur parce que toutes ces informations changées peuvent avoir d'être contaminées et donc avec le DNSSEC que on va vous le montrer dans une seconde, Ogwina est capable de distinguer entre les fausses informations et les faux serveurs et les bonnes informations, elle le fait avec la fumée bleue et le DNSSEC le fait avec les clés et autres et les signatures, donc avec le DNS il n'y a pas de réelle sécurité et ce protocole a été créé en 82 et 83 avant même la création d'Internet, et à l'époque les chercheurs n'avaient pas pensé à cet élément de sécurité et donc il n'y a pas de sécurité. Il s'agit donc de contamination d'espèces, et dans ce cas vous avez ici l'adresse originelle

à gauche et vous avez à droite la fausse adresse. Donc comment on fait cela avec le DNSSEC? Il s'agit d'un concept de signature numérique, vous créez une paire de clés où il y a une clé publique est une clé privée, la clé publique la clé privée pardon vous la donnait à toutes les personnes que vous voulez et vous la réservez, la clé publique étant donnée que vous pouvez stocker tout ce que vous voulez sur le DNS et les adresses, vous pouvez également stocker des clés sur le DNS c'est pourquoi que on l'appelle une clé DNS. Lorsque vous signez le DNSSEC vous créez ce que l'on appelle les signatures, vous le faites avec une clé privée et donc on peut vérifier tout cela, les signatures ce ne sont qu'une série de bits qui peuvent être stockés sur les DNS également. Donc maintenant on a des clé DNS sur les DNS et aussi des signatures sur les DNS, et dont il faut qu'il y ait un lien entre toutes ces entités et les racines.com est le lien entre la racine et com qui est l'archive DNS, et la clé racine DNS doit figurer pour que l'utilisateur sache qu'il s'agit d'informations sure. Donc le serveur racine disposait ces informations, et peux assurer que ces informations sont fiables.

La diapo suivante s'il vous plaît, donc au même niveau de connaissance depuis que nous avons étant donnés que nous avons signé ces informations et que il y a cette chaîne de conscience et de confiance entre cette racine.com, on peut faire maintenant une distinction claire entre les informations fausses que on ne peut pas signer par ce que l'attaquant n'a pas la clé privée que bigbank.com a, et on peut faire donc la distinction claire entre les informations signées et celle faussement signée. Donc tout ce que je viens vous dire en vol appliqué au même schéma que je vous ai mentionné auparavant, puis-je inviter de nouveaux mes compagnons de me rejoindre ici?

ROOT: Bonjour à tous, je suis la racine est d'abord il faut signer la racine. Donc je vais le signer moi-même et me voici et voici ma clé est maintenant il faut que je change ma clé avec.com, bonjour parce que vous êtes réellement.com?

COM: Oui je suis vraiment.com.

ROOT: Dans ce cas-là on peut changer nos clés.

.COM: Merci.

ROY ARENS: Ca c'est un échange de clés, ce que l'on vient de faire envoie le refaire.

.COM: Bonjour je suis.com, est-ce que vous êtes réellement bigbank.com?

BIGBANK.COM: Oui je le suis.

.COM: Parfait, alors voilà votre distinction.

ISP: Maintenant l'adresse de BigBank.com est signée.

JOE USER: On va parler maintenant des transactions DNS, mais ce fois nous avons la même transaction et plus de factures. Donc www.bigbank.com. Mr ISP?

ISP: Vous voulez aller à bigbank.com, je ne sais pas où s'est étendu de poser la question autour de moi et j'ai besoin de parler à la racine et je vais demander la clé publique de la racine et je sais où il se trouve et je lui pose la question alors est-ce que vous savez où se trouve BigBank.com?

ROOT: Oui je sais, il se trouve à 1.1.1.1. Et attendez je vais signer cela pour vous.

ISP: J'ai vérifié la signature que vous m'avez donnée, il est en compatibilité avec la clé que vous m'avez donnée.

ROOT: Et lorsque vous parlez avec lui le chiffre est trop lent.

ISP: Merci 1.1.1.1. Bonjour.com, je veux aller à www.bigbank.com et je ne sais pas où il se trouve?

COM: Je ne sais pas où il se trouve mais je sais où il se trouve à l'adresse 2.2.2.2, voilà la signature qui correspond à cette information est également la clé de bigbank.com.

ISP: Alors les clés et les signatures correspondantes tout était en ordre. Il faut maintenant que je demande à bigbank.com.

DR. EVIL: Moi je connais la réponse à cette question, c'est 6.6.6.6.

ISP: Merci beaucoup, laissez-moi vérifier la clé. Non ce n'est pas la bonne clé.

BIGBANK: L'adresse est la suivante 2.2.2.3, et voilà la signature.

ISP: Parfait, merci beaucoup, coucou Joe j'ai l'adresse et c'est 2.2.2 et les signatures correspondent.

JOE USER: Merci Monsieur le fournisseur de services Internet, nous avons donc les bonnes informations qui correspondent à ce chiffre, et la transaction va pouvoir fonctionner. L'important c'est que l'utilisateur Joe n'a rien à faire, j'ai la même demande et j'ai fait appel au même outil. Donc l'utilisateur n'a rien eu à faire de plus. Il y avait le méchant docteur Dr Evil.

PRESENTER: Merci à tous, on a essayé d'être un petit peu divertissant et je ne sais pas si vous voyez cela souvent à ICANN mais on veut être très informelle et on n'a pas encore posé de questions mais c'est une situation très informelle alors n'hésitez pas à nous poser des questions et nous essaierons de vous répondre. Donc ce que je veux vous expliquiez dans la présentation maintenant c'est de vous donner des exemples se déprécie ce des résultats de piratages qui peuvent exister sur le DNS.

JAQUES LATOUR: Après ce que nous avons vu j'ai vu qu'une personne avait un accent français, il faisait tout cela en anglais se, ce que l'on doit utiliser l'anglais bien cela s'applique aux chaînes internationalisées?

ROY ARENS: Et bien c'est supposé fonctionner avec les tous les données qui sont contenues dans le DNS qu'elle soit internationalisées ou pas. Donc vous pouvez utiliser d'autres langues et c'est tout simplement des chiffres. Et donc pourquoi s'inquiéter du DNS? À la base le DNS et le contenu du DNS doit être tout à fait correct par rapport aux applications qui sont utilisées sinon vous allez avoir des effets inattendus et néfastes également. Donc les utilisateurs finaux de l'Internet utilisent véritablement le nom DNS mais l'infrastructure qui est sous le DNS et les adresses de protocoles Internet ainsi de suite qui doive être au niveau si vous voulez que l'Internet marche bien.

Vous utilisez donc ces adresses Internet pour faire bouger les différents XXX sur l'Internet. Il y a donc des menaces de piratages au niveau des attaques DNS, vous ne voulez pas pirater le DNS en tant que telles tares ils ne vous intéressent pas mais c'est important pour les personnes qui travaillent dans le DNS mais c'est important pour les applications des utilisateurs finaux, alors que ce qui peut se passer lorsque il y a des attaques et lorsque il y a un piratage, et bien on peut dérouter ces applications et il y a de cela cinq ans par exemple ce que il y a des logiciels qui sont sur Internet et qui vous permettent de faire des piratages, il y ait des universités qui apprennent aux étudiants à faire des piratages Internet, c'est un petit peu dommage je crois et on apprend à ses étudiants de faire des côtes de piratages au DNS, c'est vraiment quelque chose que peut faire ces étudiants. Donc lorsque vous utilisez le DNS et le DNSSEC sur un site Web est bien vous pouvez utiliser les informations qui font parti du protocole pour aider les personnes à avoir si on utilise bien le système de sécurité de DNS et le DNSSEC, ce n'est pas fréquent que cela il y a plusieurs sites qui

indiquent et nous avons cette capacité qui existe et cette fonctionnalité, et lorsque l'on modifie nos sites Web, nos sites augmenteront en direct le piratage d'une partie d'un site Web et voilà comment cela peut se passer, vous avez les papiers d'information et c'est un petit peu comme les nuages qu'il envoyait au début de la présentation d'aujourd'hui et vous avez exactement l'utilisateur qui s'appelle Joe qui envoie une demande à son fournisseur de services Internet, et il y a un échange dans le réseau et un dialogue et il obtient une réponse, et la machine de l'utilisateur Joe est en mesure de converser avec le serveur de la banque, il faut qu'il y ait une réponse du DNS dans ce cas.

Lorsque vous avez un navigateur qui est conscient de l'existence du DNS, ici vous le voyez en haut le DNSSEC est coché et vous pouvez voir les requêtes qui arrivent sur ces différents sites Web qui ont la fonctionnalité DNSSEC et envoie donc coché cela est si vous n'avez pas sur votre navigateur cette capacité DNSSEC, et bien vous avez ceci club mais vous n'êtes pas sûrs de sa validité. Donc le pirate informatique il peut intercepter les messages, il observe d'une manière aucune autre les échanges et c'est assez facile à faire en fête, il observe la demande qui est effectuée par leurs utilisateurs et ce qu'il fait ce pirate informatique se situait il se place au milieu comme vous le voyez vous avez la réponse qui arrive lentement et c'est en fait le pirate qui va pirater la communication, ce qui se passe c'est que l'utilisateur sur la validation DNSSEC il peut détecter que il reçoit une fausse réponse et dont il ignore cette réponse qui n'est pas valide et qui provient d'un pirate et que elle ne provient pas de sa banque, et l'utilisateur Joe avec l'aide du système DNSSEC de la surveillance en quelque sorte réussie à communiquer et dialoguer avec le serveur de sa banque. Ça peut

devenir beaucoup plus complexe si il est beaucoup plus de serveurs car c'est un réseau.

HOSAM HASSAN: Je suis de visite, et j'ai une question et je ne parlais encore les bonnes réponses à la question que j'ai posée déjà sur d'autres personnes, le DNSSEC est bâti et c'était un rapport entre la racine et des domaines de premier niveau, mais si les clés dont on a parlé essayer un piratage de ces clés et si c'est au niveau des fournisseurs de services Internet, et au niveau de l'utilisateurs finaux. Moi il me semble qu'il y a des adresses de serveurs racines qui peuvent être piratés. Donc il y a un niveau et le piratage est possible ayant défini une route différente et un chemin différent.

ROY ARENS: Je crois avoir compris votre question, si vous êtes un opérateur qui utilise une autre racine qui n'est pas DNSSEC…

HOSAM HASSAN: Maintenant il y a un rapport avec le service et de serveurs racines, et ici vous avez le système de résolution et vous avez ici un piratage qui se déroule au niveau même du service Internet avant de sortir vers le serveur racine. Donc la question serait donc modifiée au niveau du fournisseur de services Internet, les intérêts de protocoles Internet ça peut être son serveur ou avec un autre serveur, ça va sortir de l'écosystème des domaines se est seul à avoir passé à un autre serveur.

ROY ARENS: Oui.

RUSS MUNDY: Je vais tout d'abord répéter la question je veux être sûr que j'ai bien compris. Si j'ai bien compris votre question alors qu'est ce qui se passe, le serveur racine est compromis et l'adresse IP est changée et pointe vers non pas le serveur de ICANN mais un autre serveur et par le serveur de ICANN, si la racine est compromis il y a toujours le système de validation qui existe et qui entre avec ces clés de DNS, et il y aura toujours cette procédure de validation avec la racine alternative et les réponses seront fausses et il y aura pas de validation puisque il n'y aura pas les mêmes qui s'effectuent ne correspond pas.

HOSAM HASSAN: Non il y a un piratage qui est possible au niveau du système de résolution du fournisseur de services Internet, ça peut être ont entre le serveur racine est le domaine de premier niveau et si sa pointe sur un serveur qui est en dehors de l'écosystème du DNS et qui n'appartient plus au service racine est bien à ce moment-là avec un seul clic vous allez en effet avoir un piratage.

RUSS MUNDY: Donc je regarde un petit peu l'écran que lorsque l'on a un système de résolution, c'est l'autorité du système et la résolution, si les machines du DNS ne fonctionnent pas totalement, si c'est totalement compromis

sur la sécurité du logiciel qui fonctionne bien sur ordinateur alors les résultats sont imprévisibles et à ce moment-là vous devez avoir confiance que votre xxx fonctionne bien et vous devez vous baser sur un système de fonctionnement professionnel êtes un fournisseur de services Internet ne peut pas garantir que votre ordinateur est sécurisé et cela est important pour les machines des ordinateurs de DNSSEC et doivent être solide au niveau de la sécurité avant de surfer sur Internet. Oui votre système de résolution, on peut vous monter en effet et vous pouvez utiliser votre propre système de résolution sur votre ordinateur et c'est possible ce est il y a des logiciels pour avoir votre propre système de résolution et ainsi assurer la validation de ces clés et de ces dialogues. Je crois que c'est une bonne idée d'avoir cela parce que cela vous permet d'avoir plus confiance et vous n'avez pas besoin de vous reposer totalement sur votre fournisseur Internet, et en fait si vous regardez les navigateurs jeux utilisent sur cette illustration et bien c'est ce que je fais d'ailleurs sur mes ordinateurs ce n'est pas essentiel de se baser sur la sécurité de votre fournisseur de services Internet mais la plupart des personnes pourraient le faire plus rapidement sur le fond de cette manière pour faire beaucoup mais il y a la possibilité d'avoir un système de sécurité et des résolutions sur son propre ordinateur. Donc s'arrêtant plusieurs mois à votre question j'espère.

HOSAM HASSAN: Je comprends le problème et pour être honnête avec vous j'ai du mal à obtenir la bonne réponse, comment sécuriser l'utilisateur de base et l'utilisateur final.

RUSS MUNDY: Très bien, je pense que nous allons passer à d'autres questions et nous avons continué avec notre présentation. Donc si nous avons un nouveau navigateur qui est intitulé comme Firefox si vous le connaissez et la vous avez une capacité DNSSEC. Donc il n'y a pas d'informations piratées, mais on va regarder les adresses, les adresses sont les mêmes et on demande donc les mêmes informations mais les résultats ne sont pas les mêmes et on arrive pas à la même page, la vous avez des informations piratées qui lui dit que Steve admet que le DNSSEC ne va pas résoudre la fin dans le monde et cela c'est ainsi que pirate, c'est évidemment par le site de ICANN.

Donc je regardais ici comme ces complexes avec toutes ces lignes, il y a beaucoup de demandes de DNSSEC qui existe il y a cinq ans à peu près et retardez aujourd'hui à quoi ressemble aujourd'hui xxx à cette architecture. Donc il y a beaucoup de points de demande et ce qui est important c'est d'avoir raison de donner des DNS et c'est ça qui compte, elle soit il faut que ce il faut que ce soit la bonne parce que il s'agit d'une traduction des mots de DNS dans l'adresse de réseau, compte de DNS est extrêmement important pour les utilisateurs d'Internet, il aura d'autres images que l'on pourra vous proposer et qu'est-ce qui se passe et je ne veux pas parler du flot de données, mais vous avez sur le site Web toutes ces transparents et vous pouvez utiliser ces présentations si vous le désirez, donc ici il y a les demandes et ensuite on a le DNSSEC et/ou que vous soyez dans la chaîne de dialogue au niveau du fournisseur de services Internet ou au niveau du système de résolution, vous avez vu le serveur racine et vous avez vu tous les différents rôles que ces entités jouent sur le DNS, et à ce niveau la recommandation générale et que vous devriez faire le même type d'activité lorsque vous

utilisez le DNSSEC, c'est important pour les informaticiens qui travaillent dans les entreprises par exemple, si vous êtes un opérateur de TLD ou un opérateur de registre ou un gestionnaire de registre et bien vous devez absolument travailler avec les informaticiens très compétents, si vous êtes une entreprise et vous faites appel à des sous-traitants vous devez vous assurer que ces sous-traitants soient en conformité avec le DNSSEC et c'est vraiment très important, à moins que vous vouliez avoir une expertise DNSSEC dans votre propre organisation. Donc si vous êtes un utilisateur final et vous voulez utiliser le DNSSEC aujourd'hui, eh bien si vous utilisez des Macintosh c'est très facile car c'est une plate-forme très facile à utiliser, et vous pouvez utiliser ce que on l'appelle le navigateur xxx il est très très bien pour le DNSSEC et c'est très facile donc de l'utiliser. Donc on peut peut-être donner la capacité et la qualité de la zone de données qui est absolument assurées par le DNSSEC et pour vous assurer d'avoir accès aux bonnes informations grasses ainsi que les DNSSEC et à ce système de validation qui va permettre à limiter les attaques, aux États-Unis il y a une validation DNSSEC sur tous les réseaux pour 18 millions de consommateurs, c'est un énorme fournisseur de services Internet et vous pouvez toujours le faire. Moi je suis satisfait et Google donc 8.8.8 et 8.8.4.4 font la validation DNSSEC, alors entre votre système de validation et l'ordinateur vous avait ce lien grâce à Google qui valide au niveau du DNSSEC. Donc c'est une illustration simplifiée, vous devez avoir une signature de données comme on l'a vu et elle doit être validée quelque part que ce soit sur votre ordinateur ou que ce soir sur votre serveur de validation. Donc les principes généraux dont nous avons parlé aujourd'hui, Olaf vous avait une question?

OLAF KOLKMAN: Oui, Geoff Husto de APNIC a fait de la recherche et à regarder combien d'échantillons de population étaient protégés par le DNSSEC au niveau mondial, il y a 8 % des utilisateurs Internet qui sont protégés par les utilisateurs Internet lorsque il navigue sur Internet. Donc cela c'est grâce à votre navigateur Google mais c'est un chiffre significatif d'utilisateurs d'Internet qui sont protégés par le système DNSSEC en tant que client.

RUSS MUNDY: J'ai oublié ces chiffres ils sont vraiment intéressants. Où que vous soyez et quel que soit votre système de DNS ou de noms de domaine, vous devez avoir une approche générale pour le DNSSEC et pour vous assurer qui que ce soit votre prestataire de services sur Internet, assurez-vous que vous demandiez un soutien DNSSEC ce que durant les années il y a eu beaucoup de fournisseurs de services qui se posent la question, est-ce que il y a vraiment une demande pour le DNSSEC, c'est pour cela qu'il faut demander à votre prestataire de services Internet avoir justement une capacité DNSSEC. Voici les informations que nous voulons vous transmettre aujourd'hui, et maintenant nous allons ouvrir le débat, et moi j'ai une question que j'aimerais poser, je vous ai montré ce piratage et nous avons vu même les pirates informatiques, est-ce que voudriez-vous que ce soit véritablement fait et nous pourrions avoir un réseau sans fil est piraté votre ordinateur ça vous intéresse? Parce que si quelque chose vous intéresse ne pouvant le faire lors de la prochaine réunion ICANN, ce c'est une réalité qu'on peut vraiment entrer dans un ordinateur et le piraté alors il y a des commentaires?

AUDIENCE MEMBER: Oui j'ai une question et par un commentaire. On peut poser la question? Je suis utilisatrice et je suis boursière de ICANN, et il y a donc ses systèmes de sécurité DNSSEC et j'aimerais savoir si cette chose s'applique aux applications parce que très souvent on utilise des xxx mais maintenant on utilise des applications plus que les six clubs, est-ce que les applications ont une couche sécuritaire?

RUSS MUNDY: La vous avez un exemple de piratage, vous avez un serveur DNSSEC et vous n'avez pas besoin d'avoir d'application qui sont conscientes du système DNSSEC mais c'est très utile de les avoir, vous pouvez voir le contenu, vous pouvez voir le bon contenu se est pour cela vous avez besoin d'avoir d'application et les applications qui fonctionnent avec le DNSSEC et on n'y travaille beaucoup, il y a une programmation pour les applications, il y a une interface qui est en train d'être développé qui tente justement d'avoir pour les applications un système de sécurité DNSSEC.

ROY ARENS: Moi j'ai interprété votre question un petit peu différemment. Donc les applications qui ne sont pas basées sur les sites Web avec votre iPhone ou Smartphone. Le DNSSEC et d'un indépendant de l'application, et si on l'utilise dans l'application est votre système de résolution de votre prestataire de services Internet et DNSSEC, et bien toutes les

applications vont bénéficier beaucoup, j'espère que cela répond à votre question.

OLAF KOLKMAN: Lorsque vous utilisez Internet, en fait tout ce que vous faites dans la vie la façon dont vous organisez et vous utilisez essentiellement le DNS que ce soit votre calendrier, les actualités ou envoyer un mail, ou lorsque vous passez un appel par Internet. En fin de compte tout faire appel à DNS comme une ressource pour arriver à quelque part, et tous ces éléments de menaces sont importants et si vous utilisez le DNSSEC vous faites appel à une autre couche de sécurité pour toutes ces applications qui ne sont pas forcément des choses que vous introduisez ou que vous utilisez mais qui font appel aux DNSSEC, c'est la même réponse n'est formulé différemment.

SPEAKER: Comment inscrire un ccTLD de pouvoir et met en oeuvre un DNSSEC? Et comment s'assurer que cela fonctionnait qu'elle se répartit qui ont besoin de participer et d'être impliqué?

ROY ARENS: On peut y travailler moi-même ou ccTLD on a procédé à cet exercice. Mais sachez que c'est une question très vaste, et pour y répondre j'aurais besoin de beaucoup de temps mais il n'y a rien de nouveaux ici, beaucoup de code pays il y a beaucoup d'informations à ce sujet surtout des entreprises Russ, il faut alors signer votre stand et voir si votre serveur fonctionne bien et procéder à beaucoup d'épreuves de tests par

ce que cela veut dire que si vous avez d'autres personnes qui identifient il vaut mieux que ce soit correct. Donc peut-être que il y a 10 ans c'était quelque chose de difficile à faire mais maintenant il y a beaucoup de petits et d'information de documents à notre disposition, et beaucoup de liens qui contiennent des informations à ce sujet.

RUSS MUNDY: Je voulais souligner le fait que très de un tiers des TLD sont signés dans la zone racine maintenant et ce chiffre continu d'augmenter. Et avant je vous ai dit que quelle que sois la fonction du DNS aujourd'hui que vous soyez un fournisseur TLD ou si vous êtes titulaires ou détenteurs si vos partenaires ou opérateurs, peut-être que vous êtes déjà un partenaire de registre qui est déjà en même et on dort déjà de faire un DNS est donc ce sera pas difficile de parler avec votre partenaire si il peut faire un DNSSEC pour votre zone, ou peut-être comme je l'ai dit que vous allez devoir faire la planification et la mise à l'épreuve avant de faire fonctionner ce DNSSEC.

AUDIENCE MEMBER: Est-ce que le DNSSEC a été utilisé pour les e-mails? Parce que 40 % des e-mails dans le monde ce sont des âmes. Et je travaille pour beaucoup de l'entreprise en tant que consultant qui envoie des centaines de millions d'e-mails, et les bons mails ne passent pas le filtre des spam.

RUSS MUNDY: Je crois que ce Roy qui en a parlé avant, toute application qui fonctionne sur une machine fonctionne avec le DNSSEC utilise ce

système, donc à l'heure actuelle il y a eu une mise en place d'une application qui a fait appel à SMTP et qui peut voir si le DNSSEC a été utilisé ou pas, mais ce qui se passe de plus en plus c'était au travail sur le IETF sur la technologie en conjonction avec la DNSSEC qui va permettre de renforcer ce lien SMTP.

ROY ARENS: Pour les e-mails il existe ce que on l'appelle DKIM DMARC et cela permet d'utiliser tous types de mécanismes de sécurité et en particulier le DNSSEC. Toutefois et j'adore cette citation même si ce n'est pas la mienne, le DNSSEC est une technologie qui ne résoud qu'une partie du problème, si les mails spam utilisent ce système alors on ne va pas pouvoir résoudre le problème dans son ensemble, j'espère répondu à votre question.

PAUL DONOHOE: On sait déjà rencontrer en est allé à cette conférence, merci de votre explication très simple des sujets très complexes. J'ai une série de questions que j'aimerais vous poser, la première.post est totalement DNSSEC et c'est un défi pour notre communauté surtout en temps que étant donné que le gTLDs doit être mis en oeuvre en Afrique et en Asie et en Amérique latine et il y a une adoption traînante dans l'infrastructure et dans la zone. Donc l'un des défis qui se posent à nous est l'une des questions que j'ai à vous poser c'est de quelle manière procéder pour adopter davantage d'infrastructures dans ces pays et que pouvons-nous faire pour encourager ce la diffusion de cet outil? Deuxièmement, comment en tant qu'utilisateur je peux me sentir plus à

l'aise avec l'Internet et comment je peux être sûr que c'est un espace sûr? C'est une question que beaucoup d'utilisateurs s'opposent comment être sûr que c'est un environnement sûr et comment faire ressentir cette sécurité et cette commodité? Parce que je crois que c'est l'un des principaux défis?

ROY ARENS: Je vais reformuler la première question en la rendant un peu plus générale, comment aider à l'adoption du DNSSEC dans les domaines de deuxième niveau. Alors comment les titulaires de ce domaine ont accès aux DNSSEC pour les faire signer, j'ai des cinq ce contrat avec mon opérateur de registre. Donc comment faire pour qu'ils aient cette fonctionnalité?

RUSS MUNDY: Alors vous poser la question des noms sous le.post c'est ca? Alors les opérateurs de registre sont prêts pour.post mais quelle que soit la personne qui opère que ce soit un pays et je crois que c'est très courant dans votre cas de.post ou dans notre entité, si il n'y a pas de mandat politique pour cela alors les choses se compliquent parce que comme on Roy a dit il y a beaucoup d'outils à notre disposition et donc il s'agit de savoir qu'ils existent et savoir où les trouver, et si les champs au niveau suivant en expertise suffisant de le faire mais pour faire fonctionner le DNS aujourd'hui que ce soit un service sous-traité auprès d'un autre fournisseur alors il faut trouver et il faut voir si cet opérateur est capable de faire fonctionner le DNSSEC sinon il va devoir adresser à un autre fournisseur par ce que les opérateurs essayent de défendre

leurs parts du marché en disant que ils savent fonctionner le DNSSEC, donc il s'agit de les faire avancer sans avoir recours à la carotte et au bâton.

ROY ARENS: Le deuxième aspect de la question par rapport à la première question, la Suède et les Pays-Bas qui ont été pionniers dans l'adoption du DNSSEC. Je crois que l'un des motifs de leur succès ce que il y a peu de marketing et de promotion de ce succès. Deuxième question, comment l'utilisateur final peut bénéficier de tout ce qui concerne le DNSSEC? Et comment est-ce que l'utilisateur peut voir ce qui se cache derrière tout cela? À l'heure actuelle dans la production il n'existe rien de tel, donc les utilisateurs finaux ne peuvent rien voir. Donc si il y a le déploiement de la part des fournisseurs de services Internet, il s'agit d'un mécanisme secret et j'ai entendu cet après-midi pour parler d'un projet qui était mené avec des domaines de premier niveau, afin de mettre en place un mécanisme pour voir les utilisateurs, ce que vous pouvez développer un peu le sujet Olaf?

OLAF KOLKMAN: Oui tout à fait, je suis intervenu à un certain nombre de fois semble présenter, alors je travaille pour xxx dans une petite communauté depuis plus de 10 ans maintenant pour examiner le DNSSEC et le déploiement du DNSSEC et voir comment avancer. Concernant ce que vous venez de dire, ce qu'il nous a est maintenant c'est ce que vous avez dit an dernier, comment et quel est l'interface avec l'utilisateur, ce n'est pas mon domaine de spécialisation. Les programmes actuels

d'interfaces ne s'offrent pas cette capacité, et au sein de l'IETF il y a toute une série de personnes qui travaillent là-dessus et on essaie de renforcer cette capacité mais on n'y est pas encore.

Mais je préfère ne pas intervenir ici parce que j'ai un autre point de vue par rapport à votre question, maintenant qu'ils quittent innovation avons-nous besoin pour faire la même chose au niveau mondial? Et comment innover par rapport à la structure essentielle de l'Internet? Si vous pensez à l'innovation d'une manière générale il y a des experts en marketing dans les années 60 qui se sont penchées sur ce qui motive les à prendre une décision, d'abord les avantages de la complexité ou la simplicité de l'innovation ou la compatibilité et la mise à l'essai etc. et cette capacité d'observer une innovation il s'agit de cela précisément, parce que il faut voir quel est l'avantage d'utiliser cela, DNSSEC c'est une technologie qui est nouvelle encore et donc il y a tous ces problèmes que je viens de décrire qui entraîne tous les avantages acquis ils sont difficiles à saisir, mais c'est un travail de longue haleine et on parle davantage à long terme, et il s'agit d'une sécurité à long terme pour une structure mondiale. Donc ce n'est pas quelque chose qui va être bénéfique pour vous individuellement à court terme, c'est quelque chose qui vous permet de protéger le bien-être général de l'Internet. Si on pense au niveau collectif en devrait se demander comment s'assurer que la complexité et la compatibilité soit réduite en créant des outils comme par exemple des outils pour les signatures qui sont disponibles dans beaucoup de projets en effet, un autre aspect de cet avantage c'est que en créant des mesures d'encouragement, dont les Pays-Bas vous obtenaient une subvention si vous ne signez vos droits d'enregistrement sont trouvés diminuer. Donc il s'agissait encourager

les entreprises qui avaient des centaines de noms de domaine et cela c'est vraiment très intéressant. Donc au niveau des opérateurs de registre il faut s'assurer que la communauté d'utilisateurs ont un accès facile à ces outils, et que vous pouvez leur offrir des mesures d'encouragement financier, mais ça c'est en pensant au bien-être collectif et j'espère que je vous apporte peut-être un point de vue moins technologique par rapport à votre question.

PAUL DONOHOE: Oui je suis tout à fait d'accord par rapport à ce que vous avez dit de l'infrastructure, c'est une politique sans pour 100 DNSSEC pour sécuriser les transactions, mais je voulais revenir sur ce que vous avez dit par ce que c'est l'utilisateur final qui va finalement promouvoir cette adoption mais effectivement c'est une question qui mérite d'être approfondie.

RUSS ARENS: Il y a d'autres réunions que envoie avoir mercredi, et beaucoup de thèmes qui ont été abordés vont être de nouveaux abordés d'une manière plus détail et approfondie. Comment faire en sorte que toutes ces choses-là se est que dans les ramène au niveau des utilisateurs, vous pourrez en apprendre un peu plus lors des prochaines réunions mais c'est quelque chose qui implique un changement dans les informations vis-à-vis de l'utilisateur, a-t-il d'autres questions?

SPEAKER: Quel est le changement nécessaire de la part des fournisseurs de services Internet, dans le monde il y a des millions de DNS public?

RUSS ARENS: Excusez-moi mais j'ai pas compris la question.

SPEAKER: Quel est le changement de fournisseur de services Internet afin de promouvoir la promotion de DNSSEC dans les systèmes de résolution?

RUSS MUNDY: Alors si j'ai bien compris la question cette fois-ci, je crois que la question était la suivante, que faut-il faire pour que les opérateurs de résolution dont le montant et mettent en oeuvre comment utiliser le DNSSEC. Alors l'un des aspects importants c'est que il y a une demande qui existe et tout le monde ici dans cette salle peut rentrer dans vos pays respectifs et voir ce qu'ils font les fournisseurs de services Internet, si ils ne font pas de DNSSEC parce que 8 % c'est un bon taux d'adoption, mais ça veut dire que 92 % ne l'utilisent pas. Il s'agit de faire savoir cela, et donc la demande c'est la meilleure des choses si s'agissant d'un environnement compétitif dans d'autres environnements, certains pays il y a encore un contrôle des gouvernements et une influence des gouvernements. Donc les gouvernements devraient travailler pour promouvoir l'adoption du DNSSEC.

WARREN KUMARI: Ce que beaucoup ont fait ce que cela implique un peu de travail supplémentaire mais pas beaucoup finalement. Donc ce que vous pouvez faire c'est dire à votre utilisateur et vos utilisateurs que vous

rendez les services extraordinaires en sécurisant leur travail, donc vous dites aux utilisateurs qui vous importent que vous voulez que leurs espaces Internet soient sur. Donc vous donner aux DNSSEC une valeur ajoutée et les utilisateurs vont avoir tendance à vous choisir vos, puisque vous préoccupez d'eux que d'une autre personne qui ne se préoccupait pas. Alors c'est une tactique de vente, mais certains fournisseurs de services Internet ne font et si vous ne le faites pas et s'il arrive quelque chose à vos utilisateurs on va vous demander pourquoi vous ne le faites pas et pourquoi vous ne le préoccupez pas de leur sécurité, et si vous ne le faites pas vous vous exposez à des risques et juridiques de poursuites. Depuis je veux m'assurer que j'ai bien compris cette question est peut-être que vous pourriez préciser, par rapport aux acteurs du DNSSEC, si il y a une signature de la zone racine et que le fournisseur de services Internet signe également, donc tout le domaine est signé alors qu'il d'autres intervient, par exemple dans mon pays c'est une société équitable qui permet d'avoir accès à Internet. Donc presque ils doivent mettre en place ce DNSSEC, je pensais que les serveurs de noms devraient être sûrs de quoi il s'agit.

JOYCE: On va essayer de régler les choses. Vous avez vu que toute la première partie de ce que l'on vous a montré c'était pour avoir les fonctions du DNSSEC, et M. le fournisseur de services Internet était celui qui faisait les aller retour est allé poser la question, et après cela le méchant a appris le message est il a renvoyé au bout de la file mais il aurait pu envoyer n'importe où.

RUSS MUNDY: Si il n'y a pas un système de résolution validée qui valide alors l'utilisateur ne pourrait même pas savoir si les données ont été invalidées. Donc le rôle qui est important ici pour utilisateurs finaux ce que il y a des validations de demande est d'abord il faut qu'il y ait des signatures, mais si il n'y a pas de validation des informations correctes de cette demande alors le système ne fonctionne pas se, est-ce que vous comprenez cette distinction?

JOYCE: Pas tout à fait, lorsque le domaine est signé, vous parlez des applications API, est-ce que l'il faut également signer ses applications outre nos domaines?

RUSS MUNDY: Non, les applications n'ont rien à savoir du DNSSEC temps que le système de résolution du DNS fonctionne, que ce soit sur l'ordinateur de l'utilisateur final ou du côté des fournisseurs de services Internet. C'est mieux si il le faut mais ils n'ont pas à savoir cela, y a-t-il d'autres questions? Au fond de la salle s'il vous plaît?

CRAIG NESTY: Lorsque vous avez montré le piratage, les pirates donc ne faisaient pas fonctionner de DNSSEC se est ma question est la suivante, que se passe-t-il si vous avez un serveur qui n'a pas de DNSSEC et tous les autres l'ont? Est-ce qu'il y ait une méthode compatible avec le DNSSEC?

RUSS MUNDY: La conception du DNSSEC se fait que l'on adopte les choses qui ne sont pas signées tout comme celles qui sont signées. Donc si pour obtenir la réponse aux demandes de DNS, alors on revient au point où il n'y a pas de sénateur DNS se est pour cela on peut clairement identifier dans le protocole est dans la façon dont ce protocole fonctionne si essai reconnu comme étant pas signé et donc l'information va être traitée et ce ne va pas être rejeté et ceci n'est pas censé être signé.

AUDIENCE MEMBER: Je travaille pas NIC Argentine. Donc il pourrait concevoir une application qui détecte chaque étape de la chaîne, je fais une application pour passer des appels et je veux que le programme dise que la connexion est DNSSEC, est-ce que je peux le détecter?

RUSS MUNDY: Oui, il y a des applications sur les téléphones portables maintenant et donc c'est quelque chose de faisable et si les données sont signées alors ils seront validés, donc il s'agit de voir quelle est la base de code et quel est l'application et décrire les côtes. Et nous aimerions que beaucoup d'autres gens fassent ce genre de chose si vous avez besoin d'aide, c'est une communauté qui est tout à fait disposée à aider, et en attitude de chose sur tous les personnes qui sont disposées à faire davantage dans l'environnement de DNS se, ce n'est pas une chose simple mais si vous en savez un peu plus sur cette plate-forme n'hésitez pas.

JULIE HEDLUND: Bien, il est 18:30 passé s'il en peut peut-être prendre une dernière question.

SPEAKER: Il y a une personne ici derrière les piliers qui essayaient attirer votre attention pour poser une question.

AUDIENCE MEMBER: J'ai une question, y a-t-il un rapport entre le DNSSEC et le SSL?

RUSS MUNDY: Il s'agit de deux protocoles indépendants qui se complètent, l'un travaille sans autre et vous avez plus de sécurité si vous travaillez avec les deux protocoles, mais il s'agit de deux protocoles qui peuvent fonctionner en même temps sur une même machine. Mon ordinateur n'est pas allumé mais je le fais moi-même, c'est une très bonne chose et c'est une sécurité multiple à différents niveaux. Bien je pense que nous avons fini cette réunion, excellent entraîneur et j'espère que ça se répétera et n'hésitait pas à venir nous rejoindre pour notre prochaine réunion et merci. (Applaudissements)

[FIN DE LA TRANSCRIPTION]