CR - DNSSEC for Everybody
Monday, March 12, 2012 – 16:00 to 17:30
ICANN - San Jose, Costa Rica

Julie Hedlund: Bonjour à tous! Bienvenu à vous assoir à la table pour participer, nous allons commencer dans quelques minutes. Merci.

Bien, merci à tous Veuillez entrer, il semble qu'il y a encore de la place venez vous joindre à nous, asseyez vous ici autour de la table, je pense que nous allons commencer dans quelques minutes.

[Conversation sous-jacente]

Simon McCalla: Bonjour à tous, bienvenue à cette session sur le DNSSEC. Merci de votre présence. L'objectif de cette réunion et de vous présenter une petite présentation sur le DNSSEC, pour ceux qui n'ont jamais vraiment compris ce que c'était auparavant ou pour ce que se demandent qu'est ce que c'est j'aimerais bien en savoir un petit peu plus. Bon voilà c'est une bonne session pour ça, c'est une session qui est destinée à vous apprendre quelques choses. Mais à vous amuser, vous allez voir à quoi sert le DNSSEC à quoi sert-il pour votre organisation ETC… vous avez une table, vous avez une feuille sur cette table qui va vous présenter un petit peu l'objectif

de cette réunion avec certaines ressources si vous avez besoin d'en savoir un petit peu plus sur le DNSSEC après cette réunion.

Nous allons donc vous présenter les orateurs je suis Simon. Nous sommes heureux d'avoir quelques experts du DNSSEC dans cette salle que je vais vous présenter. Donc nous somme de VeriSign, Merci Matt, nous avons [Lauras] qui est aussi de VeriSign, nous avons Matt Larsen. Une autre personne qui nous aide à déployer le DNSSEC. L'auteur ici donc d'un travail fait sur le DNSSEC. Donc nous avons des experts qui sont ici comme Norm Ritchie et qui vont nous aider et vous n'hésitez à nous arrêter s'il y a quelque chose que vous ne comprenez pas.

Donc commençons, un grand nombre d'entre vous pensent probablement que DNSSEC a été inventé à l'IETF il ya quelques années, c'était un savoir très technique, mais en réalité c'est un mensonge. Le DNSSEC a été inventé il y a 5000 ans!, en tout cas en 5000 avant JC.

Voilà c'est une dame qu'on appelle Ugwina, c'est une femme de la préhistoire qui habite le Grand Canyon. Elle est très mignonne! Et de l'autre côté du Grand Canyon se trouve son copain qui s'appelle Og qui habite donc dans une caverne de l'autre côté du Grand Canyon. Le problème qu'ils ont c'est que c'est très loin leurs grottes sont très loin l'une de l'autre. Donc ils ont du mal à communiquer, Donc un jour ils se sont réunis ils ont remarqué qu'il y avait de la fumé qui sortait de la grotte de d'un autre voisin

et ils ont eu une idée. On va faire des signaux de fumée pour communiquer d'un côté à l'autre du Canyon.

Et voilà, Hélas il y a un autre homme de la caverne qui est arrivé et qui s'appelle Komansky qui a déménagé dans la grotte d'à côté et qui a trouvé que c'était une bonne idée donc qui a commencé lui aussi a envoyé des signaux du fumé. Et donc, la pauvre Ugwina est très vraiment elle était complètement perdue à savait plus à qui appartenaient les signaux de fumé. Et donc elle a décidé de descendre au fond de ce Grand Canyon pour voir si elle pouvait résoudre ce problème. Elle est allée voir le plus sage du village qui s'appelle Diffy et Diffy a dit qu'il avait une idée assez intelligente pour résoudre le problème. Il est parti en courant au fond de la caverne de la grotte de Og et dans la grotte de Og il y a du sable qui est d'une drôle de couleur bleu c'est le seul sable bleu qu'il y a dans cette unique grotte du Grand Canyon.

Donc il a eu une idée. Il a pris une poignée de ce sable qu'il a jeté dans le feu, et la fumée est devenue bleu aussi.

Et donc maintenant Ugwina et Og peuvent parler et dialoguer tranquille puisqu'ils savent à qui appartient la fumée. Et donc Komansky lui n'a plus de, il s'ennuie parce qu'il ne peut plus les déranger dans leur conversations.

Et voilà c'est comme ça le DNSSEC, Donc rappelez vous une chose le DNSSEC c'est cette fumée bleu. Mettre quelque que chose dans la réponse du DNS pour savoir que la réponse que avez vraiment

demandé est celle qui vous parvient. Donc c'est quelque chose qui quand on parle de cette fumée bleu, rappelez-vous, hein, de cette fumée bleue.

Maintenant, nous allons donner la parole à Roy Arends de NOMINET.

Roy Arends: Je vais voir une introduction à DNSSEC. Je vais commencer par les concepts élevés et le niveau élevé du DNS.

Le DNS est un ensemble de zones. Lorsque vous voyez un nom de domaine rappelez-vous il y a des points plus le nom de domaine, le point sépare les labels entre eux ou les étiquettes si on regarde par exemple www.bigbank.com, on a donc des étiquettes de chaque côté du point, et tout cela forme un arbre.

Donc on a d'abord la zone racine, La zone racine qui ne connaît pas du tout qui c'est que la zone racine bigbank.com. La zone racine ne connaît que le TLD et les domaines de premier niveau.CR.UK, En suite on a un deuxième niveau de nom domaines par exemple.bigbang.com qui ne sait pas ce que c'est que.Com qui ne sait pat ce que c'est que les racines et comme c'est très bien séparé, tout ça donne quelque chose de très échelonnable.

Il y a un autre système qui est concerné, c'est le résolveur. Le résolveur est une partie un peu complexe parce que c'est la

machine qui fait tout le travail. Le résolveur va commencer au niveau de la zone racine et la zone racine va déléguer au résolveur, le résolveur au niveau suivant Et ETC…. Et cela avance comme ça cela s'appelle la récursion. Et cela avance jusqu'à ce que la récursion soit répondue. La récursion est rapide très rapide il y a un très grande nombre serveurs DNS, et une très grande quantité de résolveurs de DNS. Les résolveurs ont été optimisés de façon à être plus rapide en utilisant un cache. Un cache est quelque chose qui conserve l'information qui stocke l'information si vous êtes allé à bigbank.com avant, vous n'avez pas besoin d'y retourner, parce que pendant une petite période de temps cette information ne risque d'avoir changé.

Alors, vous rappelez cette image Ugwina, Hein qui parle avec Og qui est le serveur et Ugwina le résolveur va parler avec de beaucoup d'Ogs, mais en général c'est comme ça que ça marche.

Donc, je vais maintenant vous présenter quelque chose que nous allons vous présenter pour vous montrer comment fonctionne le résolveur de DNS. Donc de nouveau je vais vous montrer la zone racine. Ensuite nous allons mettre quelques.COM ensuite nous avons Russ Mundy qui va être le bigbank.com. Nous avons Norm Ritchie qui va être l'utilisateur. Et donc c'est une pièce de théâtre, et moi je vais être l'ISP, Je vais jouer le rôle de l'ISP. Pardon.

Bien. Notre utilisateur est un utilisateur (s'il vous plait un peu plus à gauche!) est un utilisateur courant « Joe User » qui veut quelque chose. Joe?

Norm Ritchie: Bonjour, je vais donc me présenter je suis l'utilisateur courant je veux aller à www.bigbank.com et je veux faire donc, je vais consulter ma banque. Je ne sais pas où se trouve cette banque j'ai besoin d'argent Donc je vais aller voir Root. Root Je voudrais avoir la route pour parvenir à ce site de la banque.

Roy Arends: Root Je voudrais avoir la route pour parvenir à ce site de la banque.

Simon McCalla: Je ne peux pas vous dire où ça se trouve mais je peux vous dire où se trouve.COM il s'agit d'un 1.1.1.1. Bien.

Roy Arends: Alors, j'ai besoin de l'adresse pour www.bigbank.com.

Matt Larsen: Je ne connais pas cette adresse, mais je peux vous dire que www.bigbank.com et son serveur se trouve à bigbank.com 2.2.2.2.

Roy Arends: Bien, bigbank.com, je voudrais la réponse maintenant, Je voudrais l'adresse de www.bigbank.com.

Russ Mundy: Bien j'ai cette adresse. Cette adresse c'est 2.2.2.3 pour www.bigbank.com.

Roy Arends: Bien, maintenant j'ai cette information et je vais vous donner cette information et redonner cette information à un autre utilisateur. Je vais la lui renvoyer.

Norm Ritchie: Merci Monsieur ISP. Maintenant, je vais retourner à ma banque, qui va être 2.2.2.3.

Roy Arends: Bien, Donc, voilà c'est comme ça que fonctionne le DNSSEC. La fonction est comme ça pendant une trentaine d'année. L'année prochaine, ça sera de 30 ans, et ce que vous venez de voir arrive vraiment dans la vie quotidienne pour entrer saisissez le nom de domaine et avant de voyez quoi que ce soit c'est très rapide. Ca fonctionne comme ça.

Mais c'est un système qui est vieux maintenant, quand il a été conçu, il n'y avait pas de sécurité sur place, et ces noms pouvaient être facilement usurpées et les caches peuvent être facilement empoisonnés. Donc pourquoi? Pourquoi ce problème? Les utilisateurs du DNS utilisaient le système UDP et non pas le TCP. Il s'agit d'un TCP d'un protocole Internet. C'est un petit peu comme quand vous téléphonez à quelqu'un, vous lui donner votre nom, la personne de l'autre côté donne son nom et, c'est comme si on serrait la main et l'information qui va circuler, vous allez la connaître.

Pour l'UDP, c'est un peu différent. Un petit peu comme si on écrit une carte postale. Quand on écrit une carte postale, vous mettez une adresse, un nom vous envoyez la carte postale, vous vous retournez et vous ne revenez plus et vous n'aurez plus de nouvel. Et quelqu'un va des fois vous renvoyer votre carte postale

Le problème, c'est qu'on ne peut pas authentifier cela seulement en regardant une adresse. On ne peut pas authentifier qui est cette personne. Donc revenons à l'histoire de l'homme de caverne Ugwina, le résolveur peut être un peu perdu, parce qu'elle ne sait pas très bien peut pas savoir qui est Og qui elle répond. Nous allons vous montrer de nouveau dans une petite pièce de théâtre. On va demander aux acteurs de venir.

Donc on va voir la même chose mais ici.

Norm Ritchie: Joe user, je dois payer mes factures. Je dois retourner à la banque

Je voudrais aller à www.bigbank.com.

Roy Arends: Merci. Je n'ai aucune information que je ne sais pas où est la racine. Et tout ça c'est.0.0.0.0. Donc je vais voir la racine. Bonjour je voudrais l''adresse de www.bigbank.com.

Simon McCalla: Je ne sais pas je ne connais pas cette adresse, mais je peux vous donner l'adresse de.COM, hein qui est.1.1.1.1.

Roy Arends: Je veux voir l'adresse de www.bigbank.com.

Matt Larsen: Je ne connais pas cette adresse, mais je peux vous donner de bigbank.com de cette adresse est 2.2.2.2.

Roy Arends: Maintenant je sais où est ce qu'elle est le serveur de bigbank.com et je voudrais demander.COM l'adresse de www.bigbank.com.

Merci bigbank.com maintenant j'ai l'adresse pour le www.bigbank.com.

Et je n'ai aucune façon de dire si j'ai vraiment l'adresse de la banque telle que je le souhaite

Norm Ritchie: Merci Monsieur ISP, je vais faire maintenant ma démarche bancaire à 6.6.6.6.

Roy Arends: Voilà de nouveau c'est comme ça qua l'on peut usurper une adresse, Ca peut aller aussi vite que le DNS en lui-même que la solution pour ce problème s'appelle le DNSSEC. Maintenant, ça se complique un petit peu, donc je vais essayer de vous expliquer le mieux possible Le DNSSEC utilise des signatures numériques pour rassurer que l'information soit correcte et arrive au bon endroit et du bon endroit. Le système de Cryptographie fonctionne comme ça. Vous avez deux clés et ces clés sont reliées l'une avec l'autre pour. L'une est une clé publique que vous pouvez donner à tout le monde est l'autre est une clé privé privée. La clé privée vous ne la donnez pas à tout le monde, vous la gardez secrète pour vous même. Parce que tout le monde sait que si vous donnez cette clé par exemple bigbank.com est associée avec cette clé. Et moi ou bigbank.com peut utiliser cette clé privée pour signer quelque chose, et le monde entier peut l'utiliser pour valider cela. Peut utiliser la clé publique pour valider cela.

Donc il y a une série de clés, une série de signatures. Et les clés publiques et les signatures sont des données, des morceaux de données, comme un texte ou une adresse Et ce qui est intéressant du DNS, c'est qu'on peut stocker ces clés et ces signatures dans le DSN et qu'on peut chercher ces données exactement comme on cherche des adresses ou autres choses ou des textes et différentes types de données.

Il y a une autre étape qui est importante et qui doit être ici indiquée. Pour que le résolveur puisse avoir confiance dans la zone racine, il faut qu'il y une transaction. D'abord on appelle ça la configuration d'une une ancre de confiance. Donc cette route est bien connue. Si vous voulez avoir une validation vous devez configurer cela et par défaut cela va s'installer et ça va vous faire un système DNS. Mais entre COM et la racine, et entre bigbank.com, il doit y avoir une étape d'authentification. Donc, la clé de bigbank.com qu'elle utilise pour sa zone doit être authentifiée par.COM et une fois que cela est fait, le.COM va placer un enregistrement de DS qui est une simple version de la clé que la bigbank utilisé.

Donc pour vous montrer cela, je vais de nouveau vous montrer une petite pièce de théâtre, et cette fois-ci, non d'abord nous allons revenir à notre diapo. Vous voyez komansky, vous voyez qu'on a le résolveur qui voit que le véritable Og qui envoie le message. Donc le DNSSEC nous aide à valider cela. Voilà, donc c'était un petit peu trop rapide.

Bien on reprend nos acteurs, revenez sur la scène. On demande aux acteurs de revenir sur scène.

Bien, alors la première étape est toutes ces zones ont besoin d'être authentifier, de s'authentifier les unes aux autres. Donc COM dois s'authentifier à Root, auprès de Root. Et ce qui se fait ici c'est l'enregistrement de DS qui est implémenté dans la zone racine. On peut maintenant avoir confiance dans.COM.

Maintenant on a confiance dans la zone racine. Et la confiance dans.com et c'est la même chose qui va arriver dans bigbank.com et COM.

Ils vont et comme j'ai maintenant la clé qui est configurée pour la racine de.COM, je peux commencer à valider.

Norm Ritchie: J'ai encore des factures à payer donc je vais aller voir M. ISP, je voudrai aller à www.bigbank.com.

Roy Arends: Je voudrai me rendre sur ce site, donc je retourne à la racine. Je voudrais l'adresse www.bigbank.com.

Simon McCalla: Je m'excuse je ne connais pas cette adresse, mais je sais qu'on a un service qui pourrait vous donner cette adresse qui est.COM.

Roy Arends: Merci! Avec cette première démarche, j'ai déjà validé une première partie. Donc je vais aller à.COM je voudrais l'adresse de www.bigbank.com.

Matt Larsen: Je ne la connais pas mais je peux vous dire que bigbank.com et son serveur se trouvent à.2.2.2.2.

Roy Arends: Parfait et de nouveau ici je peux valider cette information et c'est correct. Et Maintenant je vais aller à bigbank.com.COM, je voudrais l'adresse de www.bigbank.com.

J'ai l'adresse l'adresse, mais il y a quelque chose qui cloche: J'essaie de la valider et je ne peux pas parce que la clé n'est pas correcte. Essayons encore une fois. De le faire. Je voudrais avoir l'adresse pour www.bigbank.com.

Russ Mundy: Et l'adresse est 2.2.2.3.

Roy Arends: Maintenant je peux déclarer que je suis victorieuse. J'ai l'adresse de www.bigbank.com et donc la personne qui voulait usurper n'a pas pu le faire. Voila l'adresse de bigbank.com.

Norm Ritchie: Merci, Monsieur le ISP, Maintenant je peux faire mes démarches auprès de ma banque et merci beaucoup pour avoir déployé le DENSSEC.

Roy Arends: Voilà ça fait notre pièce ce théâtre,maintenant je vais donner la parole à Russ Mundy.

Russ Mundy: Je pense que je serai toujours dans bigbank.com et 2.2.2.2. Bien, merci à tous, On s'est bien amusé! Et j'espère que ça va vous aider à mieux comprendre de façon plus humaine quelque chose que ce fait et d'une façon que la plupart des personnes ne peuvent pas comprendre ou quelque chose qui fonctionnait et dont des gens ne sont pas conscient en tout cas. Maintenant je vais vous parler de la façon dont on peut et voir comment on imprimante le DNSSEC. Peu importe où est ce qu'on est, Si on est dans cette série d'activité du DNS comme vous le savez probablement, il y a déférentes parties qui forment le DNS, et les activités qui ont des noms, beaucoup de gens ici sont titulaires de noms ou ont un espace dans l'espace du DNS, sont propriétaires de cette espace il y a une série d'activités concernant ces noms dans le système du DNS.

Donc le DNSSEC d'une certaine façon concerne toutes ces activités. Donc si par exemple vous êtes un CCTLD, vous travaillez dans le domaine du CCTLD, vous avez beaucoup de chances de dépendre de la viabilité de ce que vous faites pour votre fonction sur DNS en lui-même, de sorte que vous aurez probablement un contrat ou des relations de contacts très solides avec des personnes qui travaillent dans le domaine du DNS est ce qu'ils connaissent le DNS Parallèlement, si le DNS est quelque chose de périphérique pour votre business, vous avez besoin du DNS de toute façon pour vos emails, donc et on a aussi des activités de DNSSEC dont on a besoin. Donc je voudrais Maintenant vous décrire la façon dont tout cela fonctionne.

Les opérateurs de CCTLD ou tout autre type d'opérateurs importants qui travaillent dans le domaine du DNS, de grandes compagnies comme par exemple HP ou IBM ont des équipes qui travaillent dans le domaine du DNS des experts et si vous êtes une compagnie qui va faire enregistrer son nom, avec beaucoup de bureau d'enregistrement qui provoquent des services additionnels, qui vont vous proposer des serveurs avec de différents noms etc.

Ici vous voyez une illustration de l'arbre du DNS, et ici vous voyez que c'est une structure qui ressemble à un arbre. Ici nous avons la plus grande entreprise HP et ici nous avons une autre entreprise du CNN.

Maintenant, CNN est un site internet très actif, et je vous donnerai des exemples, mais ce sont des business qui sont centraux et qui peuvent avoir des DNSSEC ou pas.

Maintenant si vous avez cette étape de DNS et si vous faites les fonctions vous-même pour le DNS, vous aurez probablement cette activité de DNSSEC avec ces mêmes structures. Si vous formez cela d'une façon ou d'une autre, avec des activités, vous allez le faire comme cela aussi pour le DNSSEC en tout cas, ou une partie de DNSSEC.

Donc où sont toutes ces parties du DNSSEC?

Voilà un tableau, une image, un schéma, C'est quelque chose que j'ai fait il y a quelques années pour une réunion de l'ICANN, aussi pour essayer d'illustrer le contenu du DNS et vous montrer que c'est la partie importante lorsqu'on vous a présenté notre petite pièce de théâtre on avait la bonne adresse IP, pour la donner à l'utilisateur, et on essayait de ne pas se laisser usurper cette adresse.

On peut appeler cela le titulaire le registrant que vous voyez ici on a les bureaux d'enregistrement qui peuvent ne pas être présents dans la zone mais qui sont extrêmement communs, on a beaucoup de bureau d'enregistrement dans la plupart des zones

Les registres, chaque TLD a un registre. On est obligé d'avoir un registre pour que cela fonctionne. Ensuite, il y a l'opération du

nom de serveur, et chaque zone doit avoir une opération d'un nom de serveur. Très souvent, cela est lié à un service existant. Mais les gens ont tendance à penser automatiquement que dans certains cas, le bureau d'enregistrement doit être son propre opérateur de nom de service. Ce n'est pas toujours le cas. C'est souvent le cas mais ce n'est pas obligatoirement le cas, Il faut que quelqu'un pour opérer tout le système du nom de serveur.

Ensuite on a le résolveur de DNS et l'utilisateur final. Vous voyez qu'il y a beaucoup d'acteurs qui travaillent et qui participent à ce processus. Donc dans un sens on monte et dans un autre on descend.

Ici vous voyez une autre illustration de nouveau avec les composantes du DNS. Ici vous voyez www comme www.bigbank.com certains doivent fournir ces informations et les mettre sur un serveur autoritatif ensuite lorsque le client pose une question par ici l'utilisateur veut obtenir cette réponse donc on a une série d'allée et venue et Joe va recevoir sa réponse.

Si Maintenant on a une entreprise plus grande. Voilà une illustration:

Ca était fait pour une version antérieure de DNS.COM ici vous voyez une constellation de nom de serveur qui sont ici, qui figurent ici.

Et Voilà une illustration d'un outil qui a été développé pour faire une carte, un schéma des réponses du DNS. Ça était fait il y a quatre ans et ici combien de requêtes il faut pour remplir une page web, voilà vous le voyez ici ce n'est pas seulement une seule requête ou deux ou trois, si on a un grand site comme cela ; il y a énormément de demandes de requêtes et la complexité continue à augmenter et si vous voyez il y a 6 mois toujours le même site internet. Donc un énorme nombre de requêtes DNS, c'est ce qu'on disait toute à l'heure cela arrive essentiellement en un clin d'œil combien de temps ça vous prend lorsque vous allez à CNN.COM pour avoir une réponse c'est très rapide et toutes ces requêtes peuvent avoir lieu avant ou en même temps que la page web apparait sur votre écran donc la chose importante que je voulais vous montrer içi ce sont les données qui se trouvent dans le DNS: le nom les adresse IP et les informations concernant cette adresse IP, c'est ca qui compte, et de ça qu'il s'agit quand on parle de zones DNS.

Lorsqu'on parle de sécurité du DNS quelques soit les parties dont on parle, quelque chose qui est importante à sa voir c'est que c'est toujours les données su DNS qui sont les plus importantes Il s'agit de DNSSEC sui a été créé pour protéger ces données DNS donc comme vous l'avez vu sur la pièce de théâtre une personne peut venir essayer d'usurper cette adresse et données mais cette donnée est protégée. Parfois on met l'accent sur la protection de DNS à travers un système cryptographique. En fait cela vise à

protéger les données qui sont dans la zone DNS. Je vous ai montré dans toutes les parties à gauche vous voyez sur l'écran ce qu'on appelle le secteur d'approvisionnement, C'est le secteur dans lequel on a les données qui vont être saisies dans le DNS, et d'ans l'autre partie droite il s'agit du fonctionnement du DNS. Et ici c'est les choses que le DNSSEC protège dans le sens propre du terme.

Et du côté gauche il y a des choses qui doivent être faites par rapport ou à travers le DNSSEC. Si vous vous rappelez on avait deux personnes qui se serraient la main, qui s'étaient donné la confiance en haut de la cela doit avoir lieu avant que le mécanisme de fonctionnement puisse utiliser ces données et sortir de l'arbre, les données vont donc avoir un flux qui va être dans ce sens et le DNSSEC va fonctionner su doté de fonctionnement de la machine si vous voulez.

En général comme je l'ai dit que l'on trouve sa place ans cette image de l'ensemble de la structure du DNS et lorsqu'on se demande ce qu'on fait, je vais vous donner une série d'exemple.

On va probablement utiliser la même approche qu'on a utilisée aujourd'hui, c'est-à-dire qu'on a un contractant qui va vouloir utiliser tout cela, donc si vous opérer un grand système d'opération de DNS, vous aurez probablement l'intention ou la volonté d'utiliser les produits qui existent et que vous utilisez couramment et incorporer l'utilisation du DNSSEC par exemple le système qui soutient et qui supporte le DNSSEC et nous avons eu

une réunion avec Microsoft la semaine dernière. Microsoft fais de grand progrès, ils ont des fenêtres de données, ils savent ce qu'ils font.

Dans cette ligne de produit il y a beaucoup d'autre systèmes de produit Open sources, et propriétaires qui sont disponibles et il y a une autre activité qui est très intéressante en tout cas pour moi, j'aime beaucoup le DNSSEC c'est le système ou service de signature

Si aujourd'hui on travaille dans le secteur des opérations de DENSSEC et pour une certaine raison ça ne peut pas être viable. On ne peut pas faire de changement dans votre registre ou dans votre serveur de noms, on a la structure de nom ou dans votre entreprise, on peut à ce moment la prendre les données de votre zone autoritatif les zones envoyée à VeriSign ou Nominet ou à un autre qui va faire la signature des données pour vous, et qui va vous renvoyer les données de façon à ce que ayez d'avantage de fichiers (un fichier plus grand en tout cas) et vous n'aurez pas besoin de faire de modification dans votre système en lui-même au-delà de la possibilité d'avoir le flux de données qui rentraient dans votre serveur de données envoyées au système de serveur de signatures et qui va vous le renvoyer ensuite à votre serveur de noms. Et comme je l'ai dit ce que vous faites peut être un mélange de tout cela, de tout ce que je viens de vous mentionner

Donc si on utilise des produits d'un vendeur. Et je ne mentionnerai pas de vendeur en particulier, nous avons une enquête de produit de DNSSEC il y a beaucoup de produits qui ne connaissent pas le DNSSEC et ça c'est un problème. Donc si vous avez un de ces produits et que vous allez voir avec votre vendeur et vous lui dites est ce que vous avez un DNSSEC? Il va vous dire Oh excusez-moi je ne peux pas vous donner ce type de produit. A ce moment-là vous avez le choix, vous pouvez utiliser les différents produits et faire pression sur votre vendeur pour qu'il vous en parle, ce n'est pas comme d'autres caractéristiques que l'on peut aller voir un vendeur et vous lui dites non on fait pas ça actuellement, mais ce que je le recommande c'est de le réclamer, en tout cas une des choses qu'on entend concernant le DNSSEC c'est que « nos clients ne nous le demandent pas » donc allez voir aux vendeurs réclamer le dites leur je veux cette fonction parce que beaucoup le font mais beaucoup d'autres ne le font pas.

Il est aussi possible que dans cet environnement le service de signatures puisse aussi être utile en cet instant, mais c'est quelque chose qui va fonctionner moins bien quand vous contrôlez toute votre opération. Donc si vous êtes le propriétaire, le titulaire d'une série de nom, j'ai des registres qui ont différent nom de marques je dois dire que je ne sais même pas quelle est la totalité des noms que je possède je sais que beaucoup d'autres ont déjà entendu des entreprises dire qu'elles ont des centaines de noms qui sont titulaires de centaines de noms, et donc on doit à

nouveau examiner ce qu'on fait avec la gestion de ces noms des noms qu'on l'on a enregistré il faut réfléchir sur la façon dont on va pouvoir faire entrer ces noms dans le DNS comme signatures ou comme zones signées.

Donc si vous avez un enregistrement. Vous allez demander à ce bureau d'enregistrement quand est ce qu'il peut commencer à vous faire offrir ce service de signatures ou d'opérations de noms de service signé, et si vous opérez si vous fonctionnez votre propre serveur de noms, et vous allez donc offrir ce service, devoir offrir ce service à l'intérieur de votre entreprise, c'est une situation similaire mais il faut considérer ce que l'on doit faire, et voir qu'elle est donc la situation générale pour pouvoir vraiment en arriver au point ou lorsque les données sont signés dans la zone ils ont un DNSSEC. Et à ce moment-là, le résolveur récursif validant peut obtenir l'information qu'il a besoin pour valider de nouveau et cela pour l'utilisateur final.

Donc voilà la fin de la présentation. Pour voir les approches de haut niveau pour ce que vous devez faire et je pense que Simon va assumer maintenant dans le rôle de modérateur pour la séance de question. Je pense que vous avez bien compris, mais je vais redonner la parole à Simon.

Simon McCalla: Merci Russ. D'abord je vais faire une question à tout le monde ici demander dans la salle Est-ce que ça vous été utile? Est-ce que

vous avez appris quelque chose de nouveau? Ou alors Est-ce qu'on aurait dû parler ou mentionner des aspects que l'on pas mentionné.

Julie Hedlund: Oui, oui rapprochez-vous de la table! S'il vous plait. On a des micros ici. Et si vous voulez parler servez-vous du micro SVP parce que l'on enregistre la session et ça va nous aider à mieux entendre au même temps.

« Voilà poussez le bouton vert! »

Pedro: Merci je m'appelle Pedro, je suis de Costa Rica, je peux savoir davantage sur le DNSSEC. Est-ce que ceci est inclus sur l'IETF? Si vous avez versions préliminaires sur le document ou est-ce que cette version est finale ou c'est une fonction préliminaire est-ce que ça fonctionne ETC? Merci.

Roy Arends: Je suis Roy Arends, Matt et moi (Matt est là-bas dans la table) avons travaillé pour la standardisation de la DNSSEC et donc le DNSSEC est un standard. Il s'agit d'un standard internet selon l'IETF on l'appelle un standard proposé. La plupart des standard IPF sont proposés. Et en fait, ceci veut dire qu'il s'agit d'un projet qui est bien mis en place. Il s'agit d'une bonne pratique, si vous

voulez vous servir de ceci, si vous voulez le chercher et ses 40 30 33 et 35 et vous pouvez nous parler moi et Matt après.

Simon McCalla: Oui, on a une autre question au fond de la salle.

Male En fait, l'authentification entre les serveurs des domaines de haut niveau et les serveurs comme on voit est fait, mais, ma question est qui authentifie le serveur de haut niveau lui-même. Est-ce que le résolveur doit revenir au serveur de racine et il n'y a pas d'authentification à ce niveau, Mais après ceci on a l'authentification entre le serveur racine et le serveur pour le domaine de haut niveau.

Male 2: Et bien, donc sur le DNSSEC on n'a pas de concept d'authentification le serveur fait simplement l'authentification de données.

Roy Arends: Donc en ce moment, la requête de l'utilisateur est envoyée au serveur racine. Donc comment est-ce qu'on peut garantir que le serveur va arriver à ce serveur racine qui contient les données qui vont l'amener à l'autre branche de l'arbre? Mais en fait on n'a pas de garantie lorsqu'on envoie une question pour savoir qu'on va

revenir au serveur indiqué. Donc on n'a pas de garantie rien n'assure que votre question va être répondue par un serveur normal. Mais en fait, vous recevez l'information cryptographique. Et donc ceci authentifie la transaction. Donc, ça n'importe pas d'où vient l'information. Il s'agissait de la correction des données et d'authentifier les données, est en fait indépendamment d'où elles viennent, de la zone racine ou de la zone de site et en fait on peut se rassurer qu'on a les bonnes données. Donc c'est indépendant d'où ça vient.

Male: Merci.

Simon McCalla: Alors je vais vous demander combien parmi vous travaillent avec la mise en place du DNSSEC, voilà on considéré la mise en place du DNSSEC pour votre organisation. Est-ce que quelqu'un se trouve dans cette situation?

Bien, nous avons quelques personnes qui sont dessus et alors où en êtes-vous par rapport à la mise en place du DNSSEC. Est- ce que vous le considérez ou vous avez déjà commencé? Oui, oui racontez-nous.

Male: En fait on a commencé, on a sous-traité la plupart de nos DNS et on a enregistré et donc on a peut-être pas de DNSSEC et sur le serveur alors on est en train de migrer sur un autre serveur pour pouvoir le DNSSSEC. Au même temps on a nos propres serveurs de noms qui travaillent avec le DNSSEC.

Simon McCalla: Et donc est ce que c'est difficile pour vous ou c'est simple de faire cela. Vous avez les bonnes ressources?

Male: Oui, oui nous avons l'information dont on a besoin. Donc certains personnes ; je pense que ce soit bon pour le client parce qu'on fait le service de sécurité. Et donc on leur fournit aussi une partie de ce service au même temps.

Simon McCalla: Mais c'est très bien. Alors pour le reste vous en êtes où? Pour la mise en place du DNSSEC?

Victor: Je suis Victor di Salvador on va le prendre et va le considérer tout simplement. Je voudrais demander quelque chose que vous avez dit. Vous avez mentionné la possibilité d'envoyer, d'avoir une zone qui soit signée par une autre personne, un tiers et le récupérer, Je veux savoir combien de temps prend cette

possibilité en termes de minutes et quelle est la sécurité que ceci garantie?

Simon McCalla: Je pense que c'est une question pour Matt qui vient de VeriSign.

Matt Larsen: Ceci varie selon les serveurs mais la plupart sont très rapide il s'agit de quelques munîtes ou quelques secondes même. Et en générale ils se servent de signatures de transactions et ce type de protocole pour garantir la transaction. Et donc ceci garantie que la communication entre vous et le serveur sont dans la même zone et donc vous savez que vous recevez les informations de la zone indiquée.

Simon McCalla: Donc je voudrai signaler qu'en fait on a beaucoup de services de signatures mais en ce moment plusieurs organisations, quelques-unes sont des organisations petites. Le VeriSign est un service d'authentification en même temps. Ce serait bon de mettre en place ceci si particulièrement on n'a pas les ressources pour travailler avec le DNSSEC vous-même vous pouvez chercher une organisation qui sous-traites ceci et c'est une bonne option. Et donc, plusieurs personnes voient ceci comme un pas intermédiaires ça les aident à commencer à travailler avec le

DNSSEC pendant qu'elles considèrent comment on va mettre en place ceci dans leurs organisations.

Est-ce qu'on a d'autres commentaires? Est-ce qu'on a d'autres personnes qui sont en trains de considérer l'utilisation du DNSSEC. Qui sont déjà en mettre en place ce DNSSEC?

Louis [Fulan]: Bonjour, je suis Louis [Fulan] de [dot JT], j'ai dit entraide de changer l'ingénie de notre logiciel parce qu'on a eu le même logiciel pour 10 ans c'était pour la plupart manuel. Et en fait, on considère l'inclusion du DNSSEC en ce moment, Mais pour l'instant c'est juste une idée.

Simon McCalla: Est-ce que vous êtes en train de penser à faire le DNSSEC vous-même ou alors de le sous-traiter. Comment est-ce que vous considérez ceci?

Louis [Fulan]: En fait on considère les deux options, on a des études de ceci qui vient de l'université mais on ne sait pas si on a à faire avec eux. Donc on analyse d'autres options.

Simon McCalla: Parfait Merci. Oui, va-y.

Male: J'ai une suggestion pour vous, puisque vous pensez à un processus de changement d'ingénierie de logiciel, vous devrez considérer les produits que ce soit les libres ou payant ETC. vous devriez chercher qu'ils puissent supporter le DNSSEC actuel c'est même avec le service de signatures vous allez travailler avec les serveurs de noms qui doivent pouvoir supporter adéquatement les RFC actuelles ; donc pour les services de signatures c'est un grand pas intermédiaire pour pourvoir commencer à travailler avec ceci. Si vous n'avez pas les services de signatures. Donc ils doivent pouvoir travailler avec les fonctionnalités du DNSSEC.

Louis [Fulan]: Merci c'est une excellente suggestion.

Simon McCalla: Est-ce qu'on a quelqu'un ici qui soit préoccupé de mes avis DNSSEC ou qui pense que ce n'est pas une bonne idée?

On a entendu de parler des gens qui le considèrent. Mais est- ce qu'on a des gens qui pense que je n'ai pas de bonne idées ou qui sont préoccupé par voilà la mise en place? D'accord ; je considère comme on n'a pas de préoccupation. Je vais faire une question aux membres ici du panel. Est-ce que vous devriez, Si vous deviez donner des conseils à des personnes qui commencent à travailler avec ceci quelles sont types de conseils que vous leurs donnerez?

Roy Arends: Je travaillais à plusieurs étapes de la mise en place du DNSSEC et on fait j'ai vu toutes ces étapes. Donc si vous voulez mettre en place le DNSSEC à l'heure actuelle ne le considérez trop. On a beaucoup de serveurs qui travaillent avec le DNSSEC comme l'open DNSSEC c'est un des outils que Russ Mundy a mentionné. Et on fait vous avez travaillé vous-même faire l'ingénierie de votre côté. Mais il y a beaucoup d'information sur la taille de la clé, sur la signature fréquente ou non fréquente. Et donc vous allez faire ce que font les serveurs hauts niveau ce que font les serveurs racine. Et ça fonctionnera. Donc servez-vous d'information les plus récentes. Sur la zone signée. Vous pouvez faire signée la zone racine. Et en fait, tout marchera, vous verrez. Merci.

Simon McCalla: Matt.

Matt Larsen: Je crois qu'on a beaucoup de ressources qui vont nous aider. Mais je vois ici que nous avons beaucoup d'informations et écrites sur le DNSSEC publié pour savoir comment il fonctionne, comment le mettre en place. Je pense que beaucoup de gens seront contents de vous aider à mettre en place toutes ces ressources, de vous les faciliter. L'une est facilité de mise en place le DNSSEC l'autre est le DNS Og. Le centre de recherche d'analyse du DNS ainsi donc vous allez répondre aux questions spécifiques sur le DNSSEC que vous pourriez avoir.

Simon McCalla: Merci Matt. Russ est ce que t'a des suggestions?

Russ Mundy: En fait je pense que je suis d'accord avec ce qu'avez dit et donc je conseille de ne pas réinventer la roue. En fait, cherchez les informations disponibles et adéquates pour votre situation. On a beaucoup de gens avec lesquelles on a parlé ces derniers temps. Et apparemment les gens mettent beaucoup d'énergie et consacrent du temps à réinventer quelque chose qui existe déjà. Donc servez-vous des ressources existantes et vous verrez quand on a beaucoup de gens qui seront content de répondre à vos questions. Et donc suivez les étapes de façon pas à pas. Et n'essayez pas de changer tout le système DNSSEC et de le mettre en place ensemble parce que vous voulez le remplacer.

Si vous voulez remplacer le système DNSSEC, DNS allez-y faites-le. Mais ceci n'implique pas un changement énorme c'est tout simplement parce que vous allez changer le DNS. Vous pouvez le faire pas à pas et vous servir de ce que vous avez déjà.

Norm Ritchie: En fait je voulais répéter ce qu'on venait de dire. Ce n'est pas un domaine dans le quelle il faut innover. Il y a beaucoup de personnes qui ont déjà travaillé dessus. Les gens intelligents qui ont pensé à tout et qui sont content à vous aider.

On a des références standard pour le DNSSEC il faut voir si votre système puisse supporter le DNSSEC plus actuel 5.9.9 est compatible avec plusieurs systèmes.

Simon McCalla: Oui, va-y ROY.

Roy Arends: Je vais ajouter que depuis le début des gens on a beaucoup d'information et les détails de réponses, est-ce que ceci n'a pas la sécurité. En fait ça ajoute la sécurité et on n'a pas de problème avec le DNSSEC et c'est ça que je voulais dire. On n'a comme ça VeriSign et kullysign. On devrait le faire On a tout les raisons pour le faire et aucune pour ne pas le faire. Merci.

Simon McCalla: Un grand Merci Roy. Alors, est- ce qu'on a d'autres questions auxquelles vous voulez qu'on répond? Ou que vous avez toujours des doutes? Oui, Allez-y.

Louis [Fulan]: Oui, merci je ne me suis pas présenté. Je suis de Costa Rica je voudrais savoir comment le DNSSEC fait la signature des communications lorsqu'une clé a été usurpée? Comment est-ce qu'elle fonctionne avec le système DNSSEC? Comment agit-elle par rapport à ça?

Roy Arends: Le DNSSEC est différent de TLS ou de système de certification. Donc le DNSSEC n'a pas de système de vérification plus que le temps.

Par exemple, pour les registres signés vous avez une signature qui a une marque de temps (de l'heure). Alors, l'idée et de maintenir les délais aussi court que possible.

Donc le délai sert à, aussi court que possible pour vous assurer que ne prendra pas tout le temps. Donc et celle-ci aura expiré si ça prend beaucoup de temps. Ça prend au maximum deux jours.

Simon McCalla: Donc si vous avez un problème avec la clé ou vous ne pouvez pas la récupérer ; donc par rapport à la mise en place ceci sera propagé dans votre DNS. Donc ce n'est pas ce que vous allez le récupérer.

Très bien donc si on a plus de question. On a une journée entière d'information sur le DNSSEC. Ce sera Mercredi prochain. Je pense que c'est à partir de 18h30.

Julie Hedlund: Oui c'est mercredi à 8h30 dans la salle « la passé ». Donc c'est juste en haut. Et on va avoir une mise à jour régionale. On a beaucoup de gens qui sont en train de mettre en place le DNSSEC.

On a des exemples donc vrais de partout dans le monde et beaucoup d'information utiles. Donc, je vous invite à venir. Et on aura un repas un déjeuner à la fin. Don peut être que ceci va vous inviter un peu plus. Merci. Donc on vous attendre à mercredi. Il y a des opportunités à discuter ceci, le DNSSEC. Je remercie mes collègues d'avoir organisé cette session d'aujourd'hui. N'hésitez à vous rapprocher de nous dans la fin de la session si vous avez toujours des questions. On sera ici venez nous chercher. Merci beaucoup d'être venu. ET au revoir.

[Fin de la transcription]