HYDERABAD – Réunion conjointe : Conseil d'administration de l'ICANN et Groupe d'experts techniques (TEG)
Mardi 8 novembre 2016 – 16h30 à 18h30 IST
ICANN57 | Hyderabad, Inde

DAVID CONRAD: Réunion conjointe du conseil d'administration de l'ICANN et des experts techniques, 8 novembre 2016, Hall 3 de 16 h 30 à18h30.

Pour les membres du TEG qui viennent d'arriver, je vous annonce qu'il y a quelques places devant la salle, donc si vous êtes des personnes qui veulent être ici devant, que tout le monde vous voit, venez vous assoir à table.

Nous allons commencer sous peu, dans quelques minutes. S'il y a des membres du TEG qui sont dans la salle, vous avez toujours l'opportunité de prendre place à table.

Monsieur Marby nous accompagne, nous rejoint dans la salle.

Bienvenue à tous, nous voilà réunis pour la réunion conjointe du groupe des experts techniques et du conseil d'administration de l'ICANN dans le cadre de la 57ième réunion publique de l'ICANN. Nous avons légèrement modifié l'ordre du jour qui a été publié. À l'origine on prévoyait de discuter de l'architecture des sujets, mais le présentateur, Suzanne Wolf, a indiqué qu'elle ne se sent

pas bien, donc elle promet de revenir si elle se sent mieux, mais ce n'était pas le cas. Donc on a biffé cette partie de l'ordre du jour, et nous avons maintenant ajouté la possibilité de permettre à monsieur Warren de venir nous parler des questions relatives à l'IETF.

Pour ceux qui ne savent pas ce qu'est le TEG, il s'agit d'un groupe qui se concentre sur 4 questions liées à la technologie et de la technique dans (la bande) surtout pour ce qui est du système d'identificateur unique de l'internet. Et les membres du personnel de l'ICANN, du conseil de l'administration de l'ICANN et du TEG devraient donc prendre en considération ces questions au moment de penser aux stratégies et aux opérations.

Il s'agit d'un groupe de travail, ce n'est pas un conseil consultatif puisqu'il n'a pas de budget, mais il a le rôle de conseiller le conseil d'administration. Le conseil n'est pas tenu d'accepter ces recommandations, sauf que ce sont des recommandations venues des experts, et de belles personnes ;

Cela dit, l'ordre du jour pour ce groupe de travail d'experts techniques, fournira une mise à jour sur les questions liées aux noms spéciaux. Donc on a un rapport de l'état de situation, de la déclaration du problème et de l'espace de problème tel que défini par le SSAC, c'est Jim Galvin qui va présenter cela. Puis

nous avons la virtualisation des fonctions du réseau du ETSI, qui sera présenté par Howard Benn, puis on a le DNSEXTLANG présenté par John Levine et Warren Kumari présentera les questions associées à l'IETF.

Cela dit, je donnerai la parole à Jim, pour qu'il commence.

JIM GALVIN: Merci David. Je vois que la diapo est déjà à l'écran, ce qui est très bien.

Je viens faire cette présentation aujourd'hui en ma qualité de membre du SSAC, je suis vice-président de ce groupe, mais je fais également partie du groupe de travail du SSAC qui se penche sur la question de la stabilité de l'espace de nom de domaine.

Le SSAC considère la question de l'espace des noms de domaine et la présence de noms de domaines et de conflits qui pourraient survenir en vertu de leurs utilisations au sein de la communauté internet At-Large, pour la plupart, depuis presque le début de l'année. Nous sommes venus vous présenter l'état de situation par rapport au consensus auquel nous sommes arrivés pour décrire l'espace de problèmes. Donc c'est ce que nous pensons qui est compliqué pour la communauté de l'ICANN, c'est d'intérêt pour la communauté.

Donc que veut-on dire par espace des noms de domaine ? Il s'agit de tous les noms de domaine qu'il est possible d'obtenir dans la hiérarchie des étiquettes individuelles, qui sont structurées de manière, comme un arbre.

Ce n'est pas tout simplement le DNS. Lorsque les personnes pensent au système des noms de domaines, mais ici on parle d'un sous-ensemble. L'espace de problème dans lequel nous travaillons est l'ensemble de noms de domaines qui pourraient exister dans cette hiérarchie qui suit la forme d'un arbre et le DNS ne fait qu'une partie de cette structure.

Il est intéressant d'observer dans cette communauté que l'espace de noms de domaine et le protocole du DNS qui soutient les noms de domaine gérés par ICANN et que l'ICANN délègue et attribue pour l'utilisation industrielle, sont également utilisés ailleurs. Non seulement pour le DNS public mondial.

Et c'est important de comprendre pourquoi on a des conflits.

Les noms de domaine et le DNS ont été une réussite, ce qui veut dire qu'ils ont été adaptés et adoptés pour leur utilisation ailleurs, par d'autres acteurs, ce qui est très bien. Cela montre vraiment que c'était une réussite et que ça nous donne l'occasion d'innover.

Finalement, il est important de comprendre par rapport à cet espace de noms de domaine où nous considérons le problème, c'est que les noms de domaine tels que définis aujourd'hui par l'IETF, suivant le DNS mondial, ne peuvent pas être délimités dans la pratique. C'est-à-dire que si j'ai un nom de domaine par exemple qui existe, je n'aurais pas suffisamment d'informations pour savoir quoi faire de ce nom de domaine.

Donc si vous pensez à vos navigateurs, par exemple, sur le navigateur on saisit une adresse, et un morceau de texte, et dans la plupart des navigateurs, vous avez l'occasion soit de saisir des mots pour lesquels vous pouvez faire une recherche, soit de saisir des étiquettes qui ont l'air d'être un nom de domaine et qui vont donc être recherchées dans le DNS. En termes généraux, ce n'est pas suffisant et les navigateurs doivent deviner comment le faire. Donc c'est un exemple, ils ne savent pas comment rechercher ces étiquettes.

Dans l'environnement général, on a un résolveur DNS dans l'environnement local et d'autres applications, d'autres services dans votre téléphone portable par exemple ou dans votre ordinateur, sur les laptops, ont le même type de problème.

On pourrait ne pas avoir suffisamment d'information pour savoir si le nom qui a été saisi, l'étiquette qui a l'air d'être un nom de

domaine du DNS public mondiale appartient vraiment à ce système ou pas. Et c'est ça le problème qu'on essaie d'aborder.

La communauté de l'ICANN doit être consciente de ce problème et le considérer au cours de ces délibérations.

Diapositive suivante.

Au cours de nos considérations, nous avons remarqué différentes observations concernant les circonstances et les faits que nous observons. Et nous voyons que l'utilisation non coordonnée de l'espace de nom génère des problèmes, donc on se retrouve avec des conflits ou des collisions en raison de l'utilisation non coordonnée de noms de domaines. Donc il est possible d'avoir des noms de domaine, et si on a une application qui comprend comment utiliser ces noms de domaine, il est également possible d'avoir des environnements qui sont censés faire référence à des places de l'environnement local. Ce n'est pas sensé vous renvoyer au système du DNS public mondial. C'est pour cela que l'on arrive à ce type de problème de collision par rapport aux noms de domaine.

On a ouvert une série de candidatures pour les nouveaux gTLD il y a quelques années, et dans le système actuel des nouveaux gTLD, il y a des noms qui ont été réservés jusqu'à ce que l'on sache quoi faire de ces noms. Donc HOME, MAIL, des

candidatures de noms qui ont été déposés. Il y avait également le .CORP parmi ces noms.

Cet espace de noms de domaine est utilisé dans différentes régions du monde et on ne sait pas très bien quoi faire de ces noms.

Le manque de coordination entre plus de deux noms de l'espace de noms de domaine crée des conflits. Le fait d'avoir des collisions génère une certaine ambiguïté ce qui nous amène finalement à des problèmes d'instabilité sur internet.

Donc le SSAC s'occupe directement de la stabilité de l'internet et considère ce type de problèmes, fournit des conseils pour la communauté et identifie les questions qui sont d'intérêts pour la communauté à mesure qu'elle élabore des politiques et des processus qui leur permette de travailler avec ce type de problème et ce type de système.

En ce moment il y a deux groupes qui ont de l'influence par rapport aux noms et à l'existence des noms. L'ICANN bien sûr s'occupe de cela puisque c'est l'organisation qui coordonne l'affectation et l'attribution de noms dans la zone racine.

C'est la responsabilité de l'ICANN. L'ICANN est responsable de prendre ces décisions.

L'IETF, bien sûr, est l'autre exemple évident d'une organisation qui a également un rôle, et c'est le rôle de créer une liste de noms réservés, ce sont des noms spéciaux qui doivent être réservés et reconnus pour des propos techniques. .LOCAL par exemple est un nom qui appartient à cette liste, comme .ONION.

L'IETF a ses propres processus bien sûr pour ajouter des noms à la liste. On connait tous les processus de l'ICANN par exemple qui a ses propres processus également pour permettre ou non d'exister dans la racine.

Et puis il y a d'autres individus ou institutions, il y aura sans doute d'autres qu'on ne connait pas, il y a des utilisations privées des noms de domaine, et c'est le problème de CORP, HOME et MAIL. C'est qu'il y a des utilisations privées de ces étiquettes particulières partout sur internet. C'est pourquoi ils présentent un problème, parce qu'ils sont en collision avec des noms qui pourraient éventuellement être dans la racine, dans la zone racine. Et l'ICANN, en tant que communauté, doit décider, conjointement avec le conseil d'administration et le personnel, de quoi faire par rapport à ces noms-là. Et donc c'est ce qu'il faut décider afin d'aborder cette instabilité.

Nous voilà à la fin de cette présentation de comptes rendus, qui vous montre où on en est. On a fait des présentations et des définitions de ce qui nous semble être l'espace de problèmes.

On a nos propres conclusions qui ont été tirées à partir de ce processus. Et, par la suite, nous allons élaborer une sorte de série de recommandations. Si vous avez participé à la dernière séance ici dans le cadre de la réunion de l'ICANN, nous avons fait une déclaration dans le cadre du forum public, disant que l'ICANN espère pouvoir mettre à disposition de la communauté un ensemble de recommandations formulées à travers le SSAC avant la fin de cet exercice fiscal.

Y a-t-il des questions là-dessus ?

DAVID CONRAD: Je vais donner la parole aux membres du conseil et aux membres de la communauté pour voir s'il y a des questions concernant ce sujet particulier.

STEVE CROCKER: Merci Jim, c'était très intéressant.

DAVID CONRAD: Pardon allez-y, vous pouvez prendre la parole.

PETER KOCH: Peter Koch de DENIC.

Jim, vous présentez ici une vision qui fait prétendre qu'il y a des noms de domaines, il y a un espace des noms de domaine et qu'il y a une responsabilité séparée sur le système des noms de domaine au sein de l'ICANN et une autre responsabilité au sein de l'IETF.

Et cette vision que vous présentez, c'est la perspective d'après qui ?

JIM GALVIN: Nous reconnaissons que l'ICANN a une responsabilité au niveau des noms qui sont inscrits dans la zone racine, et nous observons qu'il y a d'autres groupes qui profitent de l'existence de cette technologie, à savoir du DNS public et de son protocole de résolution, et du fait qu'il est possible d'avoir des noms qui ont été utilisés ailleurs également.

Cela dit, nous n'avons pas d'opinion par rapport à l'autorité ou la responsabilité. On reconnait tout simplement qu'ils existent et qu'ils font ce qu'ils font. Tout ce que l'on a à faire est de reconnaitre qu'ils existent. Et l'ICANN a une responsabilité envers la communauté de l'ICANN. L'ICANN est donc responsable de reconnaitre cela et de réagir par rapport à cela également.

STEVE CROCKER: Vous avez une deuxième question ?

PETER KOCH: Donc c'est qui « nous » ?

JIM GALVIN: Nous c'est l'ICAN, moi je me considère comme une partie de la communauté de l'ICANN.

PETER KOCH: Je veux dire que cette question particulière n'est pas nécessairement sans polémiques, sans conflits, et je ne serais pas tellement d'accord avec ce que vous présentez.

Vous parlez d'utilisation privée qui pourrait également dénommée squattage, donc ça veut dire que je pourrais par exemple prendre votre voiture sans votre consentement, et déclarer qu'il s'agit d'une utilisation privée de votre voiture.

L'IETF et l'ICANN ont signé un MoU qui établi une séparation claire des responsabilités par rapport à l'espace des noms de domaine, et le document à travers lequel certaines parties de l'IETF déclarent ce qu'elle croit, leur octroi le pouvoir de décider lorsqu'il y a des conflits avec les protocoles.

Donc je vois ici une certaine division et je demanderais au conseil d'administration d'aborder l'IETF pour pouvoir respecter

leurs responsabilités vis-à-vis de cet MoU. Et on pourra peut-être reprendre ces travaux sachant cela.

JIM GALVIN: Merci Peter. On prend note de votre commentaire qui sera considéré par le SSAC au moment de formuler des recommandations.

STEVE CROCKER: On continue avec une autre série s'il vous plait ?

C'est le contraire en réalité. C'est moi qui suis là à votre service.

Je ne connais pas la question à 100 %, mais je voudrais ici définir quelques questions.

Il y a d'une part ce qui est inscrit dans la zone racine, et on pourrait très bien parler du système des noms de domaine que l'on utilise pour définir ce qui est inscrit dans la zone racine. Et l'IETF a structuré l'espace des noms de domaine de sa propre manière et peut également, dans une certaine mesure, discuter de l'utilisation des noms dans des contextes autres que le DNS.

Et la question pratique qui apparait ici, est le fait que les noms sont censés être utilisés en dehors du DNS et qui apparaissent de toute façon au sein du système du DNS, donc par exemple le « hôte local », mais il y en a d'autres également.

Même si du point de vue théorique on pourrait dire que l'espace des noms de domaine utilisé pour le système des noms de domaine et le système utilisé pour d'autres domaines sont séparés, le problème est que l'on voit que les deux se confondent.

Donc plutôt que d'ignorer ce problème et de ne pas faire attention aux conséquences, il y a une autre approche qui est de dire : bien, penchons-nous sur les faits, et au cas où il y aurait des noms qui apparaissent communément pour accès à la racine et qui, bien sûr, obtiennent une réponse de domaine non existant mais qui apparaissent de toute façon, il faut le considérer comme un fait objectif de la manière dont le monde fonctionne et par la suite décidons de ce que nous comptons faire.

Est-ce que nous allons entretenir des efforts d'atténuation par rapport à ces noms, ou alors on va les interdire.

Et que je sache, l'IETF ne se concentre pas tellement sur une politique spécifique, ce n'est pas dans la nature de l'IETF, on ne pourrait pas leur dire quoi faire, mais typiquement l'IETF essaye de contourner les problèmes de politique.

Donc il y a différentes factions, je sais qu'il y en a qui disent : l'IETF devrait pouvoir s'exprimer par rapport à ce squattage et à l'utilisation de noms. C'est comme l'exemple que vous dites,

c'est comme d'entrer dans un terrain privé qui n'a pas été assigné ou qui n'est pas de la propriété d'une personne spécifique, ce n'est pas comme dans le cas de la voiture.

Donc ONION par exemple, est un exemple raisonnable de cela.

Or, comment s'intègrent toutes ces composantes à votre avis ?

PETER KOCH: Oui, merci de corriger mon analogie. Par exemple, si quelqu'un occupe ce terrain, « occupe » ce n'est pas un terme extrême, mais s'il est occupé, il n'est plus disponible pour les autres, et c'est là que commence à interagir ce problème avec la coordination.

Mais je pense que la responsabilité ici devrait être claire, ce n'est pas une question d'ignorer les faits ou le trafic, comme pour les adresses IP faussées par exemple qui existent.

Et personne ne semble réagir de la manière dont vous suggérez. Donc personne ne peut déclarer sa propre adresse ou déclarer qu'une adresse est de sa propre propriété et puis que, puisque ça fait tellement longtemps qu'il s'en sert, et bien finalement cette adresse est devenue la propriété de cette personne.

Ce que je tiens à dire ici est que dans le document de l'IETF il y a un conflit clair parce qu'il n'y a pas de coordination entre les

deux organismes. Donc si ça a l'air d'être un nom de domaine, c'est probablement un nom de domaine, c'est ça que l'on se dit.

Et à mon avis, il faut que l'on établisse clairement les responsabilités, et ce n'est pas le cas à l'heure actuelle.

WARREN KUMARI: Oui, permettez-moi de vous répondre. On a beaucoup discuté de cette question récemment au sein de l'IETF et on a fait une déclaration du problème dans l'utilisation de l'espace de noms de domaine. On a déjà traversé le processus d'assigner un nom de domaine, qui est le .ONION.

Et il y a un certain consensus que cela n'a pas très bien fonctionné, il y a eu un processus d'adoption de l'utilisation de l'espace de noms de domaines spéciaux. Et nous espérons pouvoir conclure ce document d'ici peu pour pouvoir passer aux conclusions.

Le document dont parlait Jim, le document du SSAC, discute du besoin de coordination par exemple. Et je pense que le document de l'IETF va sans doute aborder la même question.

En ce moment vous voyez qu'il y a des discussions. L'IETF n'aborde pas l'utilisation des noms spéciaux en ce moment et nous avons également mis en pause cela jusqu'à ce que l'on sache quel est le résultat.

DAVID CONRAD: Vous avez la parole.

JONNE SOININEN : Oui, je pense qu'il faut diviser un petit peu les choses. Steve a essayé de le faire, et je pense que Jim l'a dit de façon assez éloquente. Il y a trois catégories. Il y a la racine, il y a les noms à usage réservé, et un peu ce qu'on disait, le squattage, non ? Et donc l'utilisation privée, bien sûr, cette utilisation n'est sous aucun contrôle.

En ce qui concerne les noms à usages spéciaux, il ne s'agit pas de quelque chose qui se passe au niveau de la racine, ce n'est pas résolu par le DNS. Cela est résolu par ce que l'on appelle le multicast, mais qui ne se passe au niveau de la racine.

.ONION, qui est le dernier a été alloué, et il y en a très peu qui ont été alloués, .EXEMPLE je crois… Excusez-moi ?

.ONION et .LOCAL seulement.

Mais aucun de ces noms sont résolus au niveau du DNS.

Comme le nom le dit, il s'agit de noms à usages réservés.

L'IETF a un processus pour allouer ce type de noms. Et c'est dans ce cadre que .LOCAL et .ONION ont été alloués. Et ce n'était pas

adéquat. Maintenant on travaille, l'IETF travaille sur une meilleure politique.

En ce qui concerne la coordination, quand l'IETF a commencé à travailler sur une politique pour l'utilisation de ces noms à usage spécial, une déclaration a été envoyée au conseil d'administration de l'ICANN et à la GNSO.

Je suis d'accord avec vous par rapport au fait que cela n'a pas été parfait, mais d'autre part, il y a aussi des gens de la communauté de l'ICANN et de l'organisation de l'ICANN qui participent à ce travail, et il y a une certaine coordination. Mais au niveau du SSAC, il est probable que dans leurs propositions, ils disent qu'il faut une amélioration de ces processus et qu'une plus grande coopération est nécessaire.

Mais, et je suis tout à fait d'accord avec vous, il y a un problème là-dessus, mais je ne comprends pas ce que vous dites par rapport au fait qu'il y a quelque chose d'autre en dehors de ce travail en coopération qu'il faut faire.

PETER KOCH : Sans vouloir monopoliser le micro, permettez-moi de vous répondre. Vous avez dit que c'est ce qui vient dans la racine et qui ne peut plus venir dans la racine, .ONION ou autre dans cette liste. Mais, ce document spécifique ne crée aucune restriction

pour faire quoi que ce soit au niveau de la racine ; on pourrait avoir un protocole qui pourrait affecter second niveau pour les TLD existants, et il pourrait y avoir des éléments de ce protocole qui pourraient avoir des conséquences par rapport à ces noms qui ne sont pas résolus au niveau du DNS.

Cela n'est pas arrivé encore, mais si cela peut arriver au niveau de la racine, cela peut arriver ailleurs aussi.

Alors, si on prend certaines parties de l'espace de nom et qu'on les déclare comme étant des protocoles, cela n'est pas seulement important pour la racine, pour les TLD, mais aussi pour les niveaux qui se trouvent au-dessous.

JONNE SOININEN : Oui, je pense que nous sommes tout à fait d'accord à ce que vous dites, et c'est pour cela qu'il faut qu'il y ait un dialogue et e suis d'accord.

DAVID CONRAD : Warren.

WARREN KUMARI: Oui, je pense aller dire un petit peu la même chose.

Nous avons adopté un document, l'IETF a envoyé une déclaration par le biais de son agent de liaison en disant qu'il

fallait avoir une coopération plus approfondie, l'IETF travaille là-dessus ?

Nous avons adopté un document qui est en cours. Et je m'inclus dans ce travail. Je pense que nous essayons de progresser, je suis un peu étonné de certaines de vos déclarations.

JONNE SOININEN: Si vous me permettez, l'ICANN, la communauté de l'ICANN, travaille aussi sur cette question. Bien entendu, il y a des points à améliorer, mais nous sommes déjà au travail.

RON DA SILVA: C'est un bon dialogue, mais si j'ai bien compris, vous parlez d'un travail entre l'IETF et l'ICANN, mais on travaille sur un espace de noms de domaine où il y a aussi des consommateurs, des entreprises, et il y a des noms de domaine qui se ressemblent beaucoup dans ce DNS.

Donc vous avez parlé des adresses et cela me fait penser aux espaces qui existaient avant les registres. Et ces adresses qui n'ont jamais été utilisées avant, certaines personnes peuvent s'en servir pour des usages internes au niveau d'une entreprise. Et c'est le même problème, il peut y avoir des collisions qui peuvent se passer.

Quand on veut faire le routage, on se rend compte que cet espace est utilisé dans d'autres espaces privés.

Donc il y a une coordination, un aspect de coordination, mais aussi le fait d'avoir une adresse ou un espace, nécessite une coopération entre les registres, les bureaux d'enregistrements et ceux qui utilisent l'espace de nom. Et il y a des termes et des accords dans cette coopération.

Quand on a cette coopération, il n'y a pas de garantie qu'il n'y aura pas un nom qui ressemble à un autre et qui se retrouvera dans un état de collision dans l'espace de noms. Il faut s'assurer à ce moment-là qu'il y ait une coordination pour éviter cela.

Donc au niveau des noms et des adresses, on a le même type de problèmes.

KAVEH RANJBAR: Je peux comparer cela aux adresses IP. Il y a quelques années, APNIC a dû allouer quelques adresses pour lesquelles il fallait beaucoup de trafic et c'est vraiment un problème qui s'est posé à l'époque.

JIM GALVIN: Je veux définir un petit peu ce que SSAC fait. Le problème auquel nous sommes confrontés est un problème assez large.

L'IETf est un autre exemple d'organisation qui s'occupe des noms de domaine.

Notre approche par rapport aux recommandations, consiste à se dire : qu'est-ce que l'ICANN peut faire dans le cadre de sa mission ? et si c'est le cas, on se dit : essayons de coordonner les choses. C'est une recommandation assez logique. Mais tout de suite on doit se poser la question : entre qui on va coordonner et pourquoi.

Il y a beaucoup de personnes qui utilisent des noms de domaine pour des objectifs malveillants par exemple, pour squatter ou autre. Il y a donc une coordination, mais on ne peut pas établir une coordination permanente entre tous. Il faut voir avec qui et pourquoi.

L'ICANN donc doit considérer ce qu'elle peut contrôler et ce qu'elle peut faire avec les personnes avec qui elle peut travailler et coopérer.

Supposons qu'il y a donc une liste de noms qui créent de l'ambiguïté, des collisions, alors l'ICANN et la communauté de l'ICANN et le SSAC en tant que comité consultatif, doivent analyser l'instabilité qui est créée à partir du fait que d'autres personnes utilisent la technologie et que cela rentre en collision.

Alors il faut voir comment nous voulons répondre à la présence de ces autres utilisateurs qui possèdent cette liste de noms qui, de temps en temps, vont apparaitre, qui vont changer, et qu'est-ce que tout cela veut dire.

Une nouvelle organisation apparait, nous allons avoir des processus pour savoir ce que l'on doit faire. Et l'ICAN doit donc établir un processus pour pouvoir gérer ce type de situation.

Voilà la direction, voilà l'approche du SSAC. Nous voulons voir ce que nous pouvons recommander à la communauté et à l'organisation, à l'ICANN organisation.

DAVID CONRAD: Puisque SSAC s'occupe de cette question, il parait que ce serait bien pour nous de voir quelle est la recommandation du SSAC par rapport à cette question. Et voir aussi quelles seraient les recommandations des groupes d'experts techniques.

Je vais prendre note également du fait que je crois que le RFC 2860, qui est l'accord entre l'IETF et l'ICANN, dit que l'IETF a la capacité de déclarer un protocole. Mais pour les éléments qui vont au-delà des politiques qui ne sont pas adressés dans le contexte de MoU, de l'accord, ne peuvent pas être gérés.

Je vais maintenant passer au point suivant de l'ordre du jour.

Est-ce que vous pouvez remettre l'ordre du jour sur l'écran ?

Je pense que c'est Howard, oui. Très bien. Howard si vous souhaitez aborder de la virtualisation des fonctions de réseau.

HOWARD BENN: Très bien, est-ce qu'on pourrait avoir les diapos ? Prochaine diapo.

Comme vous pouvez le savoir, le ETSI, c'est l'organisation qui s'occupe des standards pour les télécommunications, c'est l'institut européen des normes de télécommunications, qui est connu surtout pour son travail dans le domaine de la téléphonie mobile.

Pendant les 10 dernières années, nous avons passé d'un monde où les téléphones portables étaient utilisés pour passer des appels à un monde où les téléphones mobiles sont utilisés pour naviguer plutôt que pour passer des appels téléphoniques. Il y a des milliards d'utilisateurs, 8 milliards de cartes SIM qui sont enregistrées et beaucoup de connectivité.

Il y a beaucoup de discussions par rapport fait de savoir comment nous pouvons mettre en valeur le travail qui a été fait dans l'industrie pendant des années, et s'en servir pour contrôler les communications plutôt que de devoir recommencer à zéro.

Alors dans le groupe du ETSI, on travaille depuis longtemps pour essayer d'élaborer des spécifications.

Il y a un certain nombre de questions qu'on a vu apparaitre. Je pensais qu'il serait intéressant d'en parler avec la communauté ici.

Nous partageons donc les installations existantes aujourd'hui, nous travaillons de concert avec les organisations comme l'IETF qui travaillent dans ce domaine.

Vous voyez là des mots que vous devez connaitre, peut-être. Nous avons donc le gestionnaire de l'entité qui veille aux fonctions de cette entité. Nous avons donc un logiciel qui fait un travail de partage des ressources, ce que l'on appelle l'orchestration. Et ces services de réseaux sont gérés pendant un cycle de vie.

Nous essayons donc d'identifier le travail qui a été fait dans la communauté de l'internet avec notre travail pour voir comment on peut utiliser ce modèle dans l'univers mobile.

Il y a plusieurs éléments qui ont pu être identifiés pendant nos discussions.

Tout d'abord la fiabilité. Et c'est intéressant de penser à la fiabilité. Nous sommes dans un moment où nous nous retrouvons encore dans un processus d'essayer de comprendre

ce que les gens souhaitent. Si le téléphone portable ne travaille pas ou ne fonctionne pas parce qu'il n'y a pas suffisamment de réseau, ils ne seront pas contents, bien entendu, mais qu'est-ce qu'ils attendent du service de téléphonie mobile ? Et les services basés sur internet, les gens veulent que les services basés sur internet puissent avoir une fiabilité de 100 %.

Je ne me souviens pas vraiment d'où viennent ces chiffres, mais la plupart des réseaux mobiles, on parle de minutes de couverture par jour.

Donc certaines des données ici nous montrent que les services sont assez fiables, mais pas tout à fait fiables.

Nous devons nous assurer également qu'il y ait une interopérabilité entre ces systèmes. Nous avons des protocoles qui permettent à différents fournisseurs de fournir différentes infrastructures, mais il faut que tout cela puisse fonctionner de manière coordonnée et que tout cela soit interopérable.

Nous avons travaillé également à des efforts de benchmarking pour ce type d'initiatives. Et nous avons également analysé la latence de ces services. Si nous fournissons des services de voix sur IP, à ce moment-là, il nous faut des périodes de latence très faibles.

Et nous travaillons notamment sur la sécurité. Il y a beaucoup d'inquiétudes par rapport au fait que si on passe des opérateurs mobiles, qui gèrent leur propre base de données, si on passe de celle-là à un autre centre qui puisse avoir d'autres systèmes fonctionnant, on est plus ouvert à des attaques, à des cyber attaques. C'est ça l'inquiétude.

Donc il y a des inquiétudes au niveau des opérateurs par rapport à cette possibilité. Il y a donc un groupe qui se penche sur cette question de la sécurité pour proposer des solutions.

Bien sûr nous devons travailler ensemble au sein de l'industrie par rapport à cette question.

Et un autre domaine intéressant. Dans le monde des communications VOIP, nous avons également une exigence dans tous les pays où nous opérons, et nous avons plus ou moins les mêmes exigences dans les pays où nous opérons et il est intéressant d'essayer de voir quelles sont les inquiétudes des différents pays en matière de cyber sécurité pour pouvoir également protéger la vie privée des utilisateurs.

La migration est bien sûr un autre domaine d'intérêt. Dans notre système actuel, les opérateurs ne veulent pas avoir de période d'indisponibilité au moment d'opérer les réseaux, et on commence à travailler de près avec la communauté de logiciels ouverts qui n'a pas l'habitude d'avoir tellement d'exigences.

Donc on commence à travailler avec les équipes de OpenStack pour essayer de résoudre ces problèmes.

Diapo suivante.

Et encore une fois, l'intégration ici est coordonnée avec la sécurité. Dans l'environnement internet, on a vu qu'il y a une virtualisation en cours depuis un bon moment et qu'il y a beaucoup de services en ce moment qui fournissent déjà des services internet où il est possible d'avoir des applications isolées d'autres, c'est ce qu'on appelle (SENDBOX), où on peut partitionner la mémoire et le stockage et où on peut s'assurer que les deux applications ne sachent pas que l'autre est là.

Il faut donc que l'on s'assure que cela est vraiment appliqué et que l'on peut garantir la sécurité.

Vous ne pouvez imaginer ce que cela donnerait que si quelqu'un accédait au réseau d'un opérateur de réseau. Je sais qu'il y a eu des problèmes par rapport au Romming de données en Inde. Mais l'un des problèmes par rapport à cette itinérance de données est le fait que l'on peut appeler n'importe quel numéro de téléphone partout dans le monde et communiquer avec tout le monde, où que ces personnes soient. Donc du point de vue de la cyber sécurité c'est bien évidement une grosse inquiétude parce qu'une personne pourrait accéder à ce réseau et porter atteinte à celui-là en très peu de temps.

Du côté des normes, nous continuons de travailler sur le développement des normes au sein du groupe qui est chargé. On travaille avec l'association GSMA, qui est une organisation au sein de laquelle tous les opérateurs de réseaux mobiles participent. Il y a des accords d'itinérance qui se font au sein de cette organisation. Il y a beaucoup de problèmes liés à la sécurité à la gestion des utilisateurs pour pouvoir gérer ces normes qui s'appliquent. Par exemple à la virtualisation des fonctions de réseau ou à d'autres domaines aussi.

Diapo suivante.

Cette diapo est la dernière je pense. Ma présentation comporte quelques autres diapositives si cela vous intéresse, mais je conclurais ici, faisant allusion rapidement au groupe de travail de sécurité de la NFB. Si vous voulez rejoindre ce groupe, il est possible d'y participer. Donc c'est un groupe de l'ISG, il est possible de participer à partir d'un formulaire qui est présenté, mais tout le monde peut devenir membre de ce groupe.

On a essayé de réunir les experts de sécurité du monde de l'internet, de la communauté des communications mobiles et également de générer un ensemble de normes à partir de nos travaux avec ces deux communautés, et de participer avec des communautés comme celles du logiciel libre, du OpenStack et

pour essayer de trouver quelle est la manière dont le mobile gère la sécurité.

Donc on transfère la sécurité de l'utilisation de cartes SIM, où il y a beaucoup de travail en cours. Donc il est possible de télécharger des crédentiels pour authentification dans un environnement sécurisé. Et on veut s'assurer qu'on peut faire de notre mieux avec ce que nous avons à porté de mains dans le domaine de la téléphonie mobile en ce moment.

L'authentification, comme vous savez, pour les personnes qui accèdent au réseau mobile, doit être faite et on sait qu'il y a des détails d'abonnement pour ces personnes-là. On ne sait pas forcement qui est cette personne, ce qui est différent du monde de l'internet où on a une connectivité très ouverte. Mais on travaille ensemble pour essayer de sécuriser l'internet dorénavant.

Merci.

DAVID CONRAD: Merci Howard, je vais maintenant donner la parole aux membres du conseil d'administration ou aux membres du public si quelqu'un a des questions pour Howard. Oui Kuo-wei.

KUO-WEI WU: J'ai un commentaire concernant la sécurité et les problèmes que nous allons devoir affronter dans l'avenir. Je pense que cela nous donne une certaine idée et j'ai certaines idées à partager avec vous de ma part.

On commence à voir les dispositifs de foyers et les différents dispositifs qui commencent à devenir populaires et de moins en moins chers dans ce cadre de l'internet des objets. Donc à vrai dire, j'ai considéré la chaine de production et l'industrie des dispositifs des maisons et voir ce qu'il se passe avec cet internet des objets. Et je vois que ce n'est pas vraiment des dispositifs qui ne sont pas chers. Les personnes doivent accéder sur internet à un site web pour obtenir un logiciel qui leur permette de gérer ces dispositifs.

Donc tous ces dispositifs et toutes ces applications de l'internet des objets font vraiment partie de ce problème de sécurité sur lequel vous travaillez.

Dans certains des pays, si vous achetez par exemple un PC ou un ordinateur Mac, ils vous donnent les logiciels gratuitement, y compris les virus. Donc je pense que les personnes qui sont ici dans cette salle savent parfaitement que les parties, les composants peuvent être achetés avec très peu de fonds et que cela nous permet de lancer une attaque DDoS. Donc c'est tout simple d'attaquer les utilisateurs de cette manière.

Et si on veut trouver un moyen de résoudre ces problèmes de sécurité, il faut absolument que l'on trouve un moyen pour que cette industrie de production agisse d'une manière qui nous permette de maintenir la stabilité et la sécurité de l'internet dans son ensemble.

Voilà mon commentaire personnel.

DAVID CONRAD: Oui ?

HOWARD BENN: J'ai une remarque à dire là-dessus. C'est intéressant ce que vous dites. On travaille depuis un moment sur des normes pour les dispositifs de l'internet des objets et il est difficile d'assurer que tous les producteurs se conforment aux directives qui sont fournies. C'est l'un des gros problèmes que l'on doit affronter dans l'avenir.

Je travaille dans un groupe qui s'appelle NGB, dont j'ai parlé à d'autres réunions conjointes et l'un des aspects sur lesquels se penchent ce groupe c'est quel serait l'avenir de l'internet si on recommençait à zéro, comment cela fonctionnerait.

À partir de ces travaux, on a vu qu'il faudrait associer avec l'internet et qu'on ne pourrait donc pas avoir des dispositifs sans

un certain type d'association. Et que par conséquent les dispositifs qui provoquent des problèmes pourraient être dissociés de problèmes sécurisés.

Donc il faut absolument faire face à ce problème, il faut établir cette limite entre la vie privée, la sécurité et l'empêchement de certaines de ces attaques. Cela devient une ligne de plus en plus fine.

Récemment, on a vu des problèmes qui sont survenus à cause du DNS dynamique, mais c'est une autre question à aborder à un autre moment.

KUO-WEI WU: Permettez-moi de répondre. Lorsque le DNS dynamique a été attaqué, l'autre jour votre ami John Klensin m'a envoyé un mail. Et vous savez qu'il y a un nombre d'années, lorsque l'IETF s'est réuni à Tapei, John Klensin a beaucoup travaillé pour essayer de connecter les constructeurs avec les membres de l'IETF et les personnes du domaine informatique. Malheureusement ce rapport ne s'est pas concrétisé. Il y avait beaucoup de dispositifs d'utilisation à la maison qui sont construits à Taiwan, en Chine pas à Taiwan, avec des composants Taïwanais. Donc John proposait d'essayer d'établir ce rapport, ou cette voie de communication entre l'IETF et les constructeurs. Donc c'était ça mon commentaire.

NON IDENTIFIE: Concernant la deuxième partie de votre réponse, parce que je pense que peut-être la première partie porte surtout sur l'internet des objets, mais on pourrait peut-être reprendre la question à Copenhague. Donc je pense qu'on devrait inviter les constructeurs qui participent aux réunions de l'IETF. Moi par exemple, je travaille pour une société de technologie et nous participons avec beaucoup de personnes. Vous savez tout le monde est content lorsqu'on participe.

Le budget pour participer aux activités de l'IETF est assez substantiel et les fournisseurs et les constructeurs se réunissent au sein de ces réunions, mais les contributions à l'IETF se font plutôt formellement par des individus. Merci.

DAVID CONRAD: Jonne, est-ce que vous voulez commenter là-dessus ?

JONNE SOININEN: Non, pas nécessairement là-dessus, c'était plutôt sur une autre partie de son commentaire concernant les NFV, mais voyons ce que veut dire l'intervenant qui est au micro.

JAY DALEY : Merci, c'est Jay au micro. Est-ce que vous pourriez m'expliquer quel est l'état de situation de la politique de propriété intellectuelle ?

HOWARD BENN : Oui, en ce moment on travaille sur les licences et sur la non-discrimination. Il y a eu beaucoup de discussions par rapport à la manière dont ETSI interagis avec la communauté des logiciels libres, parce que beaucoup de développeurs de logiciels libres ont des politiques propriétés intellectuelles libres. Ces discussions sont toujours en cours, et ce qui est clair à mon avis en tout cas, est que la communauté du logiciel libre et la communauté ETSI 3DPP, travaillent en collaboration en ce moment.

JAY DALEY : Par rapport à la question de OpenStack que vous avez abordée, cela m'a surprise un peu car il y a beaucoup de services gouvernementaux dans mon pays par exemple, qui ont en ce moment OpenStack à la base, y compris pour les dispositifs électriques.

Donc on a déjà cette barrière de confiance qui est substantielle. Je sais que les personnes de la communauté des communications ont souvent beaucoup d'exigences dans ce

domaine, mais je voudrais savoir s'il s'agit d'u code de contribution de ETSI ou si c'est un empêchement de ETSI.

HOWARD BENN: Quand à OpenStack, je dirais non. C'est simplement le groupe de travail de NFV de ETSI qui informe la communauté du OpenStack par rapport aux sujets et aux problèmes qui sont identifiés. Bien sûr, il y a des personnes individuelles qui contribuent également, mais OpenStack a toujours la même politique par rapport à la propriété intellectuelle et je pense que cela ne va pas changer.

Le seul programme qui fait objet d'une discussion en ce moment est celui autour duquel l'ETSI contribue en ce moment et je pense que c'est ça qui génère le plus de polémique au niveau du conseil de l'ETSI en ce moment.

DAVID CONRAD: Jonne ?

JONNE SOININEN: Oui, je veux rajouter un peu à cela. Je pense que ce que Howard voulait dire est qu'en fait cela génère des spécifications. ETSI génère certaines spécifications qui sont ciblées à fournir une orientation pour OpenStack ou pour OPNFV, c'est la plateforme

ouverte de virtualisation des fonctions de réseau. Et c'est une opération qui crée un cadre pour la NFV et qui contribue au OpenStack, par exemple, un des types de projets auquel cela contribue.

Lorsque je ne suis pas là, je travaille au sein d'une société, et la société de Francisco et de Howard travaillent également pour faire la même chose que moi. Nous contribuons donc avec OpenStack et NFV et on se sert des directives qui ont été accordées au sein de l'industrie de ETSI. ETSI, l'organisation des normes de ETSI a des contributions des membres qu'il suit. Donc ETSI en soi-même, ne fait pas de contribution.

Howard faisait ici allusion au fait qu'il y a un groupe qui s'appelle Open Source MANO qui est d'orchestration et de gestion d'Open Source, de logiciels libres. Et il s'agit des logiciels libres au sein de ETSI. Ils suivent ces logiciels libres, ce n'est pas un projet de sources ouvertes ou de logiciel libre, mais les membres de ETSI sont en contact avec cette initiative.

Par rapport à la présentation de Howard, je voudrais dire que concernant l'historique de la NFV ou de la virtualisation des fonctions de réseau, il y a une transition au niveau des télécommunications en ce moment, où certaines des technologies qui ont généralement été utilisées ou qui sont prêtes depuis un moment, dans ce monde informatique comme

on l'appelle, dans le nuage, dans le OpenStack en matière de virtualisation, sont également utilisés dans le monde des télécommunications et se détachent des matériels spécialisés et des éléments de réseau spécialisés, et deviennent une partie d'une architecture plutôt orientée vers les centres d'architecture et de données. Par la suite ils deviennent des matériels généralisés et puis des logiciels avec des composantes libres, mais qui pourraient également être des logiciels avec des licences qui pourraient constituer une plateforme de suivi. Auparavant, c'était un réseau plutôt discret mais qui commence à fonctionner comme des machines virtuelles ou comme un logiciel.

NON IDENTIFIE: Merci. Beaucoup d'opérateurs de télécommunication et de câbles fournissent des routeurs qui ont été remis à niveau. Et en Inde, je vois qu'il y a beaucoup d'opérateurs qui fournissent des services de large bande qui utilisent ce type de routeur qui sont réparés. Donc en matière de cyber sécurité, cela génère des problèmes pour notre région.

D'autre part, les travaux de recyclage d'électronique sont surtout communs en Asie Pacifique et en Inde. Merci.

DAVID CONRAD: Y a-t-il d'autres questions concernant le NFV ? Bien, on a une question à distance ; très bien.

REMOTE INTERVENTION: Merci. On a une question de Wolfgang (Kleinwachter) du secteur académique qui dit : les producteurs de voiture doivent se conformer à des normes de sécurité internationale. Ne pouvait-on pas faire cela pour les constructeurs de matériels et de logiciels aussi ?

DAVID CONRAD: C'est une question intéressante. J'imagine que les organisations telles que ETSI pourraient peut-être accorder des normes et des critères pour réglementer ce type de normes.

Howard, est-ce que vous voulez aborder cette question ?

HOWARD BENN: C'est un sujet dangereux je dirais. C'est une question vraiment intéressante. Est-ce qu'il faut qu'un dispositif respecte des normes et se conforme à des normes avant de pouvoir être connecté à Internet, c'est de ça que l'on discute ici. En ce moment, ce n'est pas le cas.

DAVID CONRAD: Tout à fait. Mais si on regarde les attaques de (DNS) et leurs capacités qui augmentent, ce pourrait ne pas être un autre choix dans l'avenir. Steve ?

STEVE CROCKER: Je voudrais comprendre l'affirmation de Wolfgang, dans un peu plus de détails.

Quels sont les standards ou les normes internationales et quel est le niveau de conformité qu'ils sont tenus de respecter. Je ne sais pas très bien à quoi il fait allusion.

DAVID CONRAD: Il me semble avoir compris qu'il parlait des normes automotrices, donc si une voiture peut rouler, c'est qu'elle s'est conformée à certaines exigences.

STEVE CROCKER: Ha, je n'avais pas compris cela. Les voitures sont bien plus avancées que l'internet.

Pardon, je veux dire que les voitures ne sont pas des dispositifs internet pour l'instant, n'est-ce pas.

DAVID CONRAD: Ils avancent dans ce sens.

JOHN LEVINE: C'est différent parce que dans beaucoup de pays, il faut suivre des normes et respecter des exigences pour pouvoir rouler en route et ce serait bien de pouvoir avoir une différence à ce niveau par rapport à internet.

HOWARD BENN: Bien, donc pour vendre des produits électroniques dans le marché européen, il vous fait la norme CE qui veut dire que vous êtes conforme à la norme européenne. Donc chaque téléphone portable doit être conforme aux normes européennes. En ce moment, aucun de ces documents de conformité sont en conformité avec la manière de se connecter à internet. On n'a pas de documents qui s'y conforment.

DAVID CONRAD: Bon, je pense que ce serait mieux d'avancer. Le sujet suivant est le DNSEXTLANG de John Levine.

JOHN LEVINE: Merci David. Je vois que le point de l'ordre du jour figure sur l'écran. C'est une question opérationnelle un peu différente. Est-ce que je peux avoir la diapo suivante ?

Le DNS est constitué d'enregistrements et ces enregistrements peuvent être de différents types. Il y a entre 7 ou 8 types qui sont utilisés et il y a la question de savoir pourquoi on n'a pas de nouveau type d'enregistrements.

Et ce serait donc intéressant de pouvoir coordonner ces différents types d'enregistrements ; par exemple le type DANE. Et il y en a d'autres. Paul Water a travaillé pour essayer de coordonner ce type d'enregistrements.

Nous avons un processus à 4 étapes pour faire en sorte que ces enregistrements puissent aller dans l'internet.

Tout d'abord il faut prendre les enregistrements DNS dans une espèce de fichier (maitre). Historiquement, on ajoutait le fichier de manière manuelle, avec un logiciel de traitement de texte, et ce type de méthode s'est avérée ne pas fonctionner correctement.

Ces fichiers ont été créés également dans des fichiers maitres, c'est comme un DNS un peu plus puissant. Ensuite, pour qu'une application puisse utiliser ce type d'enregistrement, l'application a une espèce de librairie qui va donc chercher dans les caches DNS pour récupérer cet enregistrement. Et c'est la façon dont a travaillé le DNS pendant très longtemps.

Quand il y a un nouveau type d'enregistrement, c'est ce qui se passe. L'IETF publie un RFC qui définit le type d'enregistrement. La mise en œuvre et la publication parfois se chevauchent. Et donc tout d'abord, il faut mettre à jour la librairie avec ce nouveau type d'enregistrement, ce qui veut dire que la personne qui maintient la librairie doit donc faire une nouvelle distribution. Et toutes les personnes qui utilisent cette librairie doivent être au courant de ce changement.

Les caches n'ont pas forcement besoin d'être mis à jour. Donc le fichier maitre doit être bien sûr mis à jour pour comprendre ce nouvel enregistrement. Les gens qui font cette mise à jour sont assez vigilants et le font assez vite, mais il faut tout de même distribuer cette nouvelle version d'enregistrement que les gens peuvent, ou pas, installer.

Et s'il y a un DNS passé sur le web vous pouvez utiliser les mêmes types d'enregistrements qui étaient utilisés il y a dix ans.

Voilà notre objectif. Nous voulons que ces trois types de parties de logiciel puissent être mis à jour de manière automatique pour les nouveaux enregistrements.

Qu'est-ce que cela veut dire ? Le serveur maitre doit comprendre la syntaxe du nouvel enregistrement et beaucoup d'autres champs. Il faut comprendre la forme binaire et donc traduire la forme textuelle en une forme binaire.

Et si vous voulez que les gens puissent trouver ces enregistrements sur le web, il faut fournir à ces gens la syntaxe correcte et les champs nécessaires.

Voilà l'idée.

Nous avons créé un langage où nous pouvons décrire les types d'enregistrements. Nous avons, au début, mis cela dans des textes, et ensuite nous avons décidé de publier cela dans le DNS pour que le système puisse, de manière automatique obtenir cette description. Et il faut donc mettre à niveau le logiciel pour faire en sorte que ces nouveaux enregistrements viennent de manière automatique, y figurent de manière automatique.

Vous voyez ce type de description, vous voyez l'enregistrement MX et vous voyez le texte où l'on voit certains champs.

Diapo suivante.

La première ligne de la description par exemple, c'est un enregistrement SRV qui est assez compliqué. Vous voyez le nom c'est SRV, le numéro c'est 33, il y a des classes pour ce type d'enregistrements. Et puis il y a un commentaire. Le premier champ c'est priorité, le deuxième c'est le poids, l'autre c'est le port et ensuite il y a le nom de domaine cible.

Et on a créé une description plus ou moins pour tous les enregistrements qui existent.

Il parait que pour pouvoir gérer des nouveaux types d'enregistrement, il y en a 14 types différents avec différentes adresses IP et différents types de champs. Et nous avons un « scape type » qui s'appelle « z » pour les moins connus. Et cela ne s'applique pas aux enregistrements que l'on utilise habituellement et cela ne représenterait pas un problème.

Dans la description des types de DNS, il y a des options. Et il parait que les options que l'on ajoute, il y en a trois. Ici vous voyez la description de l'enregistrement NSEC3. Vous prenez le champ, vous voyez il y a un algorithme H et il faut le définir comme un numéro ou bien vous pouvez le mettre dans une mnémonique.

Vous voyez donc le deuxième champ, il y a des flags, il y a plusieurs valeurs séparées par des virgules. Certains champs ont plusieurs types. Par exemple pour le SALT, c'est le quatrième champ, c'est un champ X.

Et ensuite il y a un dernier champ, qui correspond au type. Il y a certains types d'enregistrements, dans ce cas c'est des types d'enregistrements qui visent vers des noms en particulier. Et il y a une liste aussi de tous les types.

Vous pouvez regarder, lire mon document pour voir les détails. Ce que je veux dire, c'est que les options de champs ne sont pas très compliquées. Si vous lisez le RFC qui définit cela, vous allez

voir les types d'enregistrement et une description comme celle-ci vous pouvez l'avoir ou la comprendre en quelques minutes.

Est-ce qu'on peut passer à la diapo précédente ?

Cette description vous donne suffisamment d'informations pour que les librairies et le serveur maitre puissent reconnaitre ce type d'enregistrements.

Vous voyez qu'il y a des champs binaires, il y a des champs de texte et des champs binaires, et des champs B32. Avec cette description, vous avez suffisamment d'éléments pour que le logiciel d'une application puisse reconnaitre ce nouvel enregistrement.

Pour les utilisateurs, voilà où l'on voit apparaitre les commentaires. Si nous avons un utilisateur qui va définir cela dans un enregistrement Max, on va voir le type MX et après on va voir donc le commentaire. On voit qu'il y a un deuxième champ, il y a priorité, nom d'hôte et le nom du serveur. On sait quelle est la valeur des champs précédents.

Et l'utilisateur doit connaitre un petit peu de ce que l'on veut faire avec cet enregistrement. Mais c'est assez facile de comprendre et d'obtenir une syntaxe correcte.

La dernière partie consiste à obtenir les données du DNS. L'idée de Paul était de publier la description de l'enregistrement dans un endroit fixe du DNS.

Ici vous voyez donc que nous avons un enregistrement RRTYPE 999 vous voyez donc (foo record) et cela est enregistré de manière habituelle, comme vous le voyez sur l'écran. Si vous voulez l'internationaliser, il devrait ajouter des versions dans des langues locales.

Et vous voyez les chaines, la description des différents types de champs. C'est assez facile pour les logiciels de décrypter ces informations.

Quand nous définissons un nouveau type d'enregistrement, une fois que le RFC est publié, la description est placée dans le DNS et ensuite les utilisateurs peuvent la chercher dans le DNS.

Mais ce n'est pas une panacée pour tous les nouveaux types d'enregistrement. Pour deux raisons. Il y en a qui ont des syntaxes assez compliquées et qui peuvent être difficiles à être traduites dans des codes binaires. Donc on peut écrire des codes pour pouvoir arriver à cette conversion. En général tous les types peuvent être gérés par des serveurs et il ne s'agit pas de type d'enregistrements que l'on va mettre dans une zone (réalistique).

Et l'autre raison, c'est que certains nouveaux enregistrements ont besoin de mettre en place une certaine sémantique au niveau des serveurs. Quand on a un cache et que l'on cherche dans ce cache, il y a une action à mettre en place avant que cela puisse se passer, une action au niveau sémantique.

Au niveau du DNSSEC, les nouveaux enregistrements nécessitent des changements au niveau sémantique, et c'est donc une contrainte parfois.

On a inventé cela, on a commencé à le mettre en place, et David nous a aidés pour cette mise en œuvre. La spécification préliminaire est prête. J'ai modifié la librairie du DNS, la librairie (perle) du DNS. Et donc on peut aller chercher dans le DNS, chercher le type compilé dans un nouveau protocole et puis pouvoir gérer ce nouveau type d'enregistrement. Et je travaille avec les gens qui maintiennent le DNS pour voir comment on peut mettre à jour cette librairie.

Nous avons donc compilé des concepts dans (PYTON) et tout cela sera mis à disposition gratuitement.

L'idée c'est qu'une fois qu'on aura fait cela, l'ajout de nouveaux enregistrements sera facile et les gens seront plus disposés à le faire.

Nous avons très peu de nouveaux enregistrements parce qu'il y a l'impression que si on en introduit, les gens ne vont pas l'utiliser parce que la plupart des logiciels ne vont pas le reconnaitre.

Il y a beaucoup de nouveaux serveurs qui utilisent des enregistrements de textes. Et dans certains cas, ça fonctionne bien, mais dans d'autres cas, cela ne fonctionne pas aussi bien.

Je serais ravi d'en parler davantage avec les gens qui seraient intéressés et j'espère que les gens vont utiliser ceci. Steve ?

STEVE CROCKER: Merci beaucoup. C'est très, très bien, très cool. Voir cela avec le déploiement du DNSSEC et le problème d'avoir des nouveaux types d'enregistrements, Record types, nous savons qu'il y a des problèmes qui n'ont pas encore été résolus, par exemple l'utilisation des enregistrements de textes, je comprends tout à fait ce travail qui a été fait et j'apprécie énormément.

J'ai quelques questions. Par exemple le prototype, et pour l'avenir.

Deux questions pour ce qui est du succès ou de l'échec.

Une fois qu'un nouvel enregistrement est défini et que beaucoup de logiciels peuvent l'utiliser, et que cela figure dans le DNS, et

du coup, les résolveurs sont confrontés à ce nouvel enregistrement qu'ils doivent récupérer et qu'ils doivent décrypter, cela conduit à deux résultats possibles. D'un côté tout le monde le récupère du même endroit en même temps, et il pourrait y avoir des problèmes là-dessus, si on le mettait sur .ARPA il pourrait y avoir une grosse charge là-dessus.

Et l'autre possibilité, combien de temps prendrait aux résolveurs pour pouvoir répondre et traiter ce type d'enregistrement ? Je parle de résolveurs qui ont déjà une charge assez importante.

Voilà un petit peu mes questions. Et ensuite, je vois que l'on veut résoudre les problèmes auxquels nous étions confrontés par le passé à travers ce type de démarche. Est-ce qu'il y a de nouveaux types qui seraient plus susceptibles d'être utilisés grâce à cette démarche ?

JOHN LEVINE: Pour répondre à la première question, je n'ai aucune idée. Cela dépend en réalité de la stratégie de cache. Si j'ai un serveur qui est très chargé, cela va faire une différence si la librairie peut aller récupérer l'enregistrement à chaque fois.Mais je pense que c'est un détail de mise en oeuvre plutôt.

En ce qui concerne les nouveaux types d'enregistrements, il y en a plusieurs qui vont sortir et qui peuvent être facilement décrits.

Tout fonctionne bien si le nouveau type d'enregistrement utilise les mêmes champs qu'on utilisait avant. Et on a fait un répertoire de tous les différents types d'enregistrements, puis on a utilisé les champs, et on a vu que les gens utilisent certains types d'enregistrements et on a vu qu'il y avait un nouvel enregistrement EU48 et EUA64 dans les adresses Mac. Et il parait qu'il fonctionne assez bien.

Et les gens savent que c'est plus facile qu'un enregistrement soit mis en œuvre plus facilement s'ils utilisent des types de champs comme ceux utilisés avant. Merci beaucoup.

DAVID CONRAD: Non, je voudrais faire un commentaire, je pense que la réponse n'a pas vraiment répondu à la question. Vous dites qu'il ne faut pas vraiment travailler parce qu'on travaille sur un format de DNS qui est différent et donc on regarde tout simplement les numéros et qui donne une réponse de numéro binaire ; donc on n'a rien à faire par rapport aux requêtes DNS.

Tout ce qu'il y a faire c'est au niveau de ce nouveau type d'enregistrements qui vont être ajoutés aux enregistrements qui sont de la propriété d'une personne pour protéger un logiciel pour fournir ce logiciel, ce qui n'implique aucune charge au niveau du serveur.

JOHN LEVINE: Non, ce n'est pas vrai. La candidature devra décrypter l'enregistrement pour comprendre ce que l'on cherche. Si je voulais développer une application, qui utilise SMIMEA, il faudrait qu'elle sache quel est le dièse, quel est le type, quelles sont les données. Donc l'application doit savoir quels sont les champs. Mais on devrait pouvoir compiler cela une seule fois.

DAVID CONRAD : Donc si vous faisiez cela ce serait dangereux parce que vous seriez en train de mettre cela dans le DNS et ce serait vraiment très dangereux.

JOHN LEVINE: Et oui.

DAVID CONRAD: Merci.

JAY DALEY: C'est très bien John, je connais quelqu'un qui voulait essayer quelque chose du même type avec un DNS (Skima) et qui a décrit le DNS (skima) merveilleusement, et tous les différents types de champs et tout ce qui est compris dans le DNS étaient compris dans ce système en davantage de profondeur.

Quelques commentaires là-dessus, d'une part comment comptez-vous internationaliser la manière dont les informations sont présentées en tant que données binaires ? Comment vous allez le faire pour le présenter aux utilisateurs finaux ?

JOHN LEVINE: Je pense que les enregistrements individuels pourraient avoir d'internationalisation que dans le cadre des chaines, des champs de chaines qui vont être présentés aux utilisateurs.

JAY DALEY: Donc dans le cadre des champs.

JOHN LEVINE: Oui, les adresses IP n'ont pas besoin d'être internationalisés. C'est une bonne question. Mais c'est également un sujet auquel personne n'a pensé.

Les registres de texte et les chaines sont à reprendre à zéro. On peut développer quoi que ce soit. Mais que je sache, personne ne fait cela. Donc la réponse serait si on trouve au niveau de l'IETF qu'en fait on va avoir des données qui ne correspondent pas au type inscrit ASCII dans le DNS, ils vont trouver un moyen pour décrire cela.

JAY DALEY: Oui, mais je ne parlais pas seulement de cela. Je veux dire qu'en ce moment les champs de nom n'apparaissent pas dans le DNS. Donc si quelqu'un présente ces champs à une autre personne qui choisit la langue utilisée, si ça va entrer dans le DNS, il va falloir qu'il y ait différentes versions selon la langue qui est utilisée, donc ça prend différentes dimensions et le niveau de données fournies est beaucoup plus profond également.

JOHN LEVINE: Oui, dans la version du DNS, il y a une étiquette de langue d'enregistrement.

JAY DALEY: Oui, mais la longueur de ce qui est stocké et de ce qui est codé change.

D'autre part je voulais vous dire qu'il y a ici un analogue au EPP, et ce qui se passe au sein de EPP. EPP a, au centre, un modèle de données fixes défini, et je connais quelqu'un qui a eu une bonne idée pour suggérer que l'EPP devrait spécifier un mécanisme à travers lequel de nouvelles données seraient, non pas incluses, mais décrites.

Donc on saurait de cette manière quelles seraient les données qui devaient être alimentées dans ce système. Parce que lorsque les personnes enregistrent le nom d'une société, cela doit être

fait à travers une extension. Mais si EPP travaillait à un autre niveau plus descriptif qui contenait une liste de ces champs de manière normalisée, ce serait plus simple.

Donc je suggère que ce serait peut-être bénéfique d'intégrer ces deux travaux.

Vous savez que les nouveaux enregistrements pourraient devoir être codés dans l'EPP lui-même pour pouvoir faire le transfert entre parties. Donc il y a ici un peu une contrainte de délai.

JOHN LEVINE: Oui, je ne sais pas quels sont les points communs pour la mise en œuvre, mais il faudrait le considérer.

WES HARDAKER: J'ai quelques commentaires. C'est une très bonne idée, je la trouve géniale, mais j'ai quelques demandes. N'ajoutez pas le format d'internationalisation dans l'enregistrement lui-même parce qu'il y a plein d'aspects différents. Ajoutez-le à l'étiquette, donc si je veux trouver l'anglais, je ne vais demander qu'une seule réponse plutôt que d'avoir un enregistrement très long.

JOHN LEVINE: Oui, j'y ai réfléchi, mais le problème est double. D'une part comment fait-on en cas de défaillance, comment le fait-on

comme paramètre normal, par défaut. Mais au-delà de cela, si on veut bien le faire, j'ai un exemple pour les codes de langage en deux lettres : l'anglais est EN et ça ajoute le pays, il y a plusieurs pays qui utilisent le EN, et ils sont connectés avec un tiret du 6. Mais il y a différents types d'informations qui ne sont pas d'importance dans les bases de données.

WES HARDAKER: Oui, ce serait beaucoup d'informations, mais pensez à cela, ce serait plus simple.

JOHN LEVINE: Oui, dans une autre version, on a ajouté l'étiquette de langue dans le nom et j'ai ajouté à l'étiquette pour simplifier un peu, mais c'est un peu plus compliqué finalement de l'avoir parmi les données.

WES HARDAKER: Oui, n'oubliez pas que récemment les tendances d'affichage dans le DNS en particulier abandonnent les bits et commencent à ajouter des mots individuels. Donc si vous voulez voir DANE par exemple, on a mis à jour cela pour qu'au lieu de voir 0, 1, 2, 3, on ait des mots clefs qui nous permettent de savoir ce que cela représente, où cela nous amène.

JOHN LEVINE: Oui c'est fait.

WES HARDAKER: Et puis, ce qui est intéressant c'est que vous pourriez peut-être avoir des questions de sécurité à appliquer au moment où il y a des problèmes de spoofing pour les enregistrements d'un bureau d'enregistrements qui utilise ce qui ne sert pas et donc finit par insérer des données dans leur zone, qui sont d'une sécurité douteuse, ou voir même de gros problèmes de sécurité.

JOHN LEVINE: Oui, c'est vrai qu'on dépend des personnes qui maintiennent ces enregistrements et ces descriptions, mais c'est le même problème que pour les bibliothèques, cela dépend du développeur (d'api).

WES HARDAKER: Oui, mais si, dans le cadre .ARPA je peux spoofer les données, ça va dépendre des applications que j'utilise parce que ça pourrait donner des résultats très différents potentiellement. Donc dans le cas des mots de passe c'est ce qui peut arriver.

DAVID CONRAD: Oui, mais on a le DNSSEC.

STEVE CROCKER: Donc si on publie une description et qu'il faut la modifier parce qu'il y a une erreur ou alors parce qu'il faut la mettre à jour, il me semble qu'il va falloir que l'on change le mot clef afin de pouvoir déclencher une mise à jour qui s'applique à tout le réseau. Autrement votre description sera utilisée à l'éternel.

JOHN LEVINE: Je n'y avais pas réfléchi vraiment. Mais c'est très rare de devoir mettre à jour ce type d'information parce que la description n'était pas la bonne ; donc j'espère si les personnes appliquent ce niveau de prudence, on ne pourra pas avoir d'erreur, c'est impossible que cela fonctionne mal.

STEVE CROCKER: Mais c'est internet…

JOHN LEVINE: Eh oui.

Vous imaginez ce que sont les étiquettes de version ou les réponses de Time out. Mais je voudrais éviter de résoudre ce problème jusqu'à ce que ce soit complètement nécessaire, parce que cela complique un peu les choses.

DAVID CONRAD: Jay ?

JAY DALEY: Oui, si vous voulez vous pourrez me demander de quitter, mais je ne sais pas très bien pourquoi cela appartient au domaine du DNS quel est le rapport avec la découverte des nouveaux RR et des nouveaux détails, puisque c'est un système opérationnel direct, je ne comprends pas pourquoi on n'a pas de fichiers statiques qui soient publiés qui permettent aux personnes d'accéder sans devoir le rechercher à chaque fois. Ce serait plus simple.

JOHN LEVINE: La mise en œuvre, telle qu'elle est en ce moment n'a pas de description lorsqu'elle voit des types de registres et cherche de trouver une description et par la suite la met en cache localement.

JAY DALEY: Donc lorsque vous voyez quelque chose qui n'est pas connu, vous allez chercher ces données.

JOHN LEVINE: C'est ça.

JAY DALEY: Très bien merci.

DAVID CONRAD: Paul, vous voulez prendre la parole ? Très bien, merci John. Nous allons maintenant passer à Warren Kumari qui va nous parler du travail qui a été fait au sein de l'IETF.

WARREN KUMARI: Merci. Je suis ici avec Paul, nous sommes les deux représentants désignés par l'IAB. Nous allons vous fournir un compte rendu de ce qui a été fait avec l'IETF.

Est-ce que ce pointeur fonctionne ? Très bien.

Cette présentation comprend deux sujets. Je vais sauter la première présentation et si on a le temps, on reviendra en arrière ou alors on passera à une autre présentation qui contient ces mêmes informations.

Donc la signalisation de confiance et de connaissance dans le DNS. Quel est le problème par rapport à la sécurité ?

En ce moment, on roule la clef de signature de clef du DNSSEC, le KSK. C'est très bien, si vous voulez d'autres informations, j'ai ajouté ici un lien, mais malheureusement le processus d'introduction de la KSK est un AFC qui s'appelle 5011, et certains systèmes ne soutiennent pas le RFC 5011. Soit parce

qu'ils sont préalables à la publication du 5011 ou ils ont choisi de ne pas le mettre en œuvre.

La plupart des mises en œuvre soutiennent le 5011, mais la plupart a le soutien du 5011 déshabilité. Parce qu'au moment où on a commencé à introduire le DNSSEC et on a fait les présentations et les ateliers par rapport au DNSSEC, on a eu un nombre d'exemples qui comprenaient le paramétrage qui disait c'est çà la zone racine, ou alors c'est ça la zone racine n'essayez pas de le changer. Et les personnes qui copient et collent cette configuration vont avoir du mal pour l'utiliser parce que ces paramètres de base ne seront pas toujours respectés avec le nouveau DNSSEC.

Ici vous voyez tous les résolveurs du DNSSEC parmi lesquels certains soutiennent le 5011 et d'autres l'ont habilité même.

Malheureusement, on ne peut pas mesurer la taille de ces cercles que vous voyez ici. Ce n'est pas vrai, on sait quelle est la quantité de résolveurs DNSSEC qui existent, mais on ne sait pas combien parmi ces résolveurs supportent le DNSSEC.

On a ici un extrait du plan de roulement du KSK qui dit en grands termes ce que j'ai dit, en termes généraux. Mais on a un document en ce moment qui va nous aider à rouler cette KSK. Il s'agit du « plan de gestion du DNSOP », c'est un plan préliminaire qui dit les choses suivantes.

Les résolveurs, de temps à autre, au moment de faire leur traitement de RFC 5010, envoient une requête qui code une liste des ancres de confiance connues. Donc dans cet exemple, nous avons une KSK avec une ancre de confiance qui s'appelle 1984, on roule le 42 42, et donc à l'origine, le résolveur envoie des requêtes pour demander le TA 1984, et lorsque le roulement de la clef commence à ce faire, cela envoie des requêtes avec le code 1984 tiret 4242. Une fois que le roulement est complet, cela va envoyer des requêtes qui contiennent TA4242 tout simple.

Cela permet aux personnes qui vérifient le trafic au niveau de la zone racine de voir quel est le pourcentage d'utilisateurs qui ont l'ancienne clef, quel est le pourcentage d'utilisateurs qui ont les deux clefs et quel est le pourcentage d'utilisateurs qui ont la nouvelle clef.

Ces mêmes informations sont codées différemment aussi et sont stockées dans une option EDNS qui est la même chose mais sous un autre code. Ce qui est bien ici, c'est qu'avant la fin du roulement de la clef, on sait qui c'est qui va avoir des problèmes et à qui on doit parler pour régler ces problèmes, pour les résoudre.

Donc est-ce que le problème est résolu ? Malheureusement, non, pas vraiment.

La mise en œuvre qui a été lancée avant le soutien de RFC5011 par définition va devoir également se mettre à jour avant la publication de ce document. C'est-à-dire qu'on ne peut toujours pas mesurer quel est le pourcentage d'utilisateurs.

Ce document fait l'objet d'une analyse de l'IETF en ce moment, il sera publié d'ici peu. On espère en tout cas.

Ça a été conclu lors du dernier appel en téléconférence du groupe, mais cela va prendre un moment pour les personnes de le mettre en œuvre en tant que code résolveur. Et une fois qu'il aura été mis en oeuvre, ça va prendre un moment avant d'être déployé.

On espère que pour le prochain roulement de KSK, on aura des statistiques un peu plus spécifiques.

Y a-t-il des questions ? Je m'excuse d'avoir été aussi rapide, mais on essaye de faire les deux présentations.

DAVID CONRAD: Steve ?

STEVE CROCKER: Oui, j'ai un commentaire lié directement avec ce que vous venez de dire par rapport à la signalisation des clefs que vous avez Ce qui me semble comparable, la signalisation par exemple des

algorithmes. Donc le fait que vous dites oui, que vous hochez de la tête me dit que le mécanisme à utiliser et la manière de le faire ont été coordonnés.

Je pense que c'est une autre discussion, mais votre commentaire par rapport à : on ne sait pas, par rapport au résolveur, on ne sait pas, etc., est similaire à la discussion que l'on a eue il y a quelque temps concernant les dispositifs connectés au réseau pour lesquels on ne sait pas quel est le statut, quel est le niveau de sécurité.

Si on a essayé d'enregistrer le dispositif dans un réseau, on sait que c'est un très grand travail, et on pourrait très bien discuter de l'enregistrement d'une sorte, ou suivant l'emplacement du DNS et des résolveurs du DNS dans le réseau, pour qu'ils puissent être contactés en cas de problème, ou qu'il y ait une certaine norme à appliquer.

Donc c'est comme de faire un jet de pierre dans un pont et de voir ce qu'il se passe.

WARREN KUMARI: Oui, on avait discuté de la possibilité de savoir quels sont les algorithmes connus, ou d'inclure la version d'un résolveur avec des algorithmes nuls, mais on a décidé de comprendre tout cela parmi tous les algorithmes potentiellement. Merci. Jay ?

JAY DALEY: Si je viens trop souvent, dites-le-moi. Il me semble qu'il y a trop de facteurs inconnus par rapport aux résolveurs d'après ce que vous dites, et je regarde David parce que ce serait bien de travailler pour comprendre quelles sont les versions des résolveurs qui faisaient chaque chose. Donc Parent Centric ou pourquoi ne pas se centrer sur les versions principales ou sur les versions en dessous, ce serait important.

Et donc on a besoin d'autres données, d'autres sondages pour voir si les sondages sont corrects en termes statistiques, on pourrait savoir quoi faire et donc apporter et extrapoler les données par rapport aux statistiques.

DAVID CONRAD: C'est un domaine actif, on s'y penche activement. Et c'est ce que nous faisons, nous faisons des recherches par rapport à la mise en œuvre des résolveurs. Et Roy analyse ces statistiques pour essayer d'informer et de comprendre l'infographique des résolveurs pour faire une carte, un plan, pour savoir quelle est la composition.

JAY DALEY: Donc on travaille sur l'identification, donc on pourrait peut-être collaborer avec vous.

DAVID CONRAD: Ron ?

RON DA SILVA: Nous allons faire un dernier commentaire concernant les statistiques d'analyse des résolveurs et ce serait bien de pouvoir avoir ce type de données, de prendre des décisions par rapport à cela.

Je me demande quelles ont été les communications proactives qui ont été engagées pour essayer d'avoir des sous-ensembles des collections de données pour les personnes qui utilisent les différents résolveurs. Comment aborde-t-on cela ? Je sais que c'est une grande lacune et on ne sait pas ce que cela va donner, quelles sont les mesures qui sont prises pour communiquer de manière proactive.

DAVID CONRAD: Pour ce qui est du roulement de KSK, on a un plan de communication assez compliqué qui est publié sur le site web de l'ICANN. /KSKROLL, je pense /plan communication ou… Vous pouvez très bien défiler dans la page, vous allez trouver cela dans notre page d'accueil.

En ce moment, nous considérons, vu qu'on a accès aux données de requêtes de refus de service pour le serveur racine. On regarde quelles sont les requêtes que nous avons reçues. Donc on regarde la source IP de ces adresses pour voir si cela amène au serveur racine, et on fait une recherche inversée pour essayer d'identifier quels sont les fournisseurs de services internet qui utilisent ces réseaux ports pour les contacter et leur dire : vous savez, il y a quelque chose de très intéressant qui sera mis en œuvre d'ici un an, donc il faudrait peut-être que vous soyez au courant.

Et nous évaluons également s'il serait possible de déterminer si le résolveur fait les questions concernant le DNSSEC, ce qui bien sûr les rendrait plus intéressants pour les résolveurs quotidiens. Mais c'est un autre type de recherches.

DANIEL DARDAILLER: J'ai une question. Est-ce que vous avez des restrictions par rapport à qui peut demander le KSK du résolveur ?

WARREN KUMARI: C'est le résolveur qui fait la publicité au niveau de la racine. Voilà. Donc cette requête est une chaine qualifiée et va pouvoir arriver au point d'ancrage. Et c'est ça ce qu'on va voir.

DANIEL DARDAILLER: Parce que s'il y a un lien entre des clefs, est-ce qu'il y a un avertissement comme quoi c'est la mauvaise clef ?

JAAP AKKERHUIS : J'ai écouté la dernière fois qu'il y a donc une espèce de cartographie des résolveurs qui est en cours.

DAVID CONRAD: Excusez-moi, qui le fait ?

JAAP AKKERHUIS: Geoff Huston.

DAVID CONRAD: Très bien. On va parler avec lui à l'occasion. Y a-t-il d'autres questions par rapport à cette question ?

S'il n'y en a pas, je pense qu'on a encore des présentations.

WARREN KUMARI: Oui, est-ce qu'on peut passer à la prochaine présentation ?

Encore une autre diapo s'il vous plait.

Cette présentation devait couvrir une demi-heure, devait durer une demi-heure. J'ai 15 minutes pour essayer de le faire. Je vais

voir si je peux résumer. Donc je vais aller assez vite. Dites-moi si je vais trop vite.

Alors le DNSSEC fournit l'authentification par des réponses positives ou négatives. Une réponse positive, vous obtenez une signature qui vous prouve que ce que vous cherchez est correct. Mais il y a aussi des réponses négatives. Donc si vous cherchez un nom qui n'existe pas, vous recevez une réponse négative du DNSSEc qui dit que cela n'existe pas et votre signature n'est pas à prouver.

En général, la signature est une opération assez chère. Donc en général, on essaye de trouver des raccourcis et on fait, à ce moment-là, des NSEC. Qu'est-ce que fait le NSEC ? Cela prend tous les noms qui existent, les range de manière alphabétique, et signe tous les espaces entre ces noms. Cela veut dire que cela ne doit pas signer les réponses forcement.

J'ai un exemple pour vous montrer. Par exemple ici, vous avez la recherche pour .BELKIN. C'est une recherche assez fréquente, voilà, .BELKIN. J'obtiens une réponse qui me dit qu'il se trouve dans X domaines. Et si je vais un peu plus bas, je vois qu'on me dit qu'il n'y a rien qui existe entre .BEER et .BENTLEY. Et il y a un ensemble de textes qui me prouve que c'est vrai. Donc mon résolveur peut chercher cela et voit que BELKIN se trouve entre .BEER et .BENTLEY.

Ce document dans l'IETF dit que les résolveurs récursives peuvent utiliser les informations des registres de NSEC. Et actuellement, si le résolveur a cherché par exemple.BELEIVE, même si cela est entre .BEER et .BENTLEY, cela va chercher encore, va lancer une recherche. Cette recherche ira à la racine, la racine donnera une réponse ; etc. Ce document dit, au lieu de faire cela, si vous savez déjà que ce nom n'existe pas, vous pouvez répondre immédiatement.

Et cela comporte des choses très positives. Cela améliore la vie privée, cela diminue le temps de réponse, parce que la réponse est immédiate, et améliore la performance bien sûr parce que le résolveur ne va pas envoyer beaucoup de requêtes.

Il y a d'autres caractéristiques qui aident à améliorer la résilience. Aujourd'hui il y a des attaques par DDos qui utilisent des noms qui n'existent pas. Ils vont au serveur récursive, le serveur récursive fait appel au serveur qui fait autorité, et cela obtient une réponse directement du cache. Le serveur d'autorité ne voit jamais ces requêtes.

Alors, est-ce que c'est utile ? vous voyez ici un exemple du 12 mai, c'était un vendredi soir, parce que c'est toujours mieux d'essayer les choses les vendredis soir, et Collin et Kaveh m'ont envoyé une question en disant que Google avait envoyé beaucoup de requêtes et qui ressemblaient à des adresses IP,

mais qui n'avaient pas vraiment la structure d'une adresse IP. Quand ils m'ont contacté, c'était minuit UTC, je ne sais pas si vous voyez le schéma, mais c'est là où le nombre de requêtes commence à augmenter.

J'ai travaillé avec Google, nous allons essayer de voir ce qu'il se passait pour voir quelle était la cause de cela, si c'était un bug, si quelqu'un avait changé le code, voir ce qu'il s'était passé, ou si on était utilisé comme un reflet DoS. Et pourquoi cela semblait être une croissance organique, et c'était ce qui nous inquiétait le plus, parce que ça n'arrêtait pas d'augmenter. Nous avons examiné, nous avions vu que ce n'était pas seulement Google qui publiait dans le DNS mais d'autres résolveurs aussi. Et on s'est rendu compte que ce n'était pas nous. Alors il fallait voir ce qui était à l'origine et comment le résoudre.

Nous avons examiné davantage, et on a vu qu'il y avait un nouveau ver qui se répandait par internet qui infectait les points d'accès et les routeurs. Ils infectaient donc une machine, un point d'accès et ensuite il lançait une recherche d'une chaine spécifique. Et cette chaine était une chaine qui était comme cela, une chaine au hasard, et des acteurs au hasard.

Nous avons essayé de voir ce que nous pouvions faire. Vous voyez ici un schéma avec les requêtes de Google aux opérateurs racine, à la racine B pardon, au serveur racine B. Et donc on voit

le schéma avant l'attaque, Google envoyait à peu près 500 requêtes par seconde. Et quand l'attaque a commencé, on est passé à 2500 requêtes, et cela a continué à augmenter.

Et c'était un vendredi, nous avons attendu jusqu'à lundi, et on a pu voir quelles étaient les réactions des machines. Nous avons attendu une machine, et puis nous avons donc relancé à 100 % toutes les locations. Vous voyez un petit peu la réaction au niveau des requêtes. 30 ou 40 requêtes par seconde au niveau du serveur racine B.

Donc que dit le document ? Si vous avez des enregistrements qui prouvent que le domaine n'existe pas, ne le cherchez pas, répondez directement que cela n'existe pas. Il y a un [Wilcard] qui peut couvrir cela, on peut utiliser donc cette information pour donner une réponse immédiate. Et voilà tout.

Donc la racine reçoit 60 % des requêtes par rapport à des noms de domaines qui n'existent pas. Si on faisait ça, les requêtes, les fausses requêtes diminueraient de 1 %.

Et voilà tout. Est-ce qu'il y a des questions ?

DAVID CONRAD: Est-ce qu'il y a des questions pour Warren ?

WARREN KUMARI: Oui, NSEC 3 ne travaille pas avec NSEC 3 sans doute parce que vous ne pouvez pas faire cela, mais pour NSEC 3, NSEC 3 travaille de manière presque identique à NSEC. Au lieu de chercher le nom qui existe, il faut ordonner tous les hashs qui existent.

RAM MOHAN: Warren, je parlais avec mes collègues qui disaient que le niveau de technicité de tout cela, qu'ils sont un peu perdus. Donc peut-être que vous pouvez synthétiser de manière plus simple quel est le problème. Cela pourrait aider.

WARREN KUMARI: Excusez-moi, je suis allé trop vite. Pour résumer les choses de manière plus simple, si cela est déployé, cela permet de diminuer le nombre de requêtes fausses au niveau de la racine. Cela augmente les performances et diminue le nombre de requêtes qui doit aller vers le serveur racine. Voilà un petit peu la synthèse. Et je n'ai pas de problème à répondre à des questions si vous voulez plus de détails.

WES HARDAKER: Bonjour, je voulais vous dire merci parce que vous nous avez aidés. Je travaille pour la racine B.

JAY DALEY: Bonjour, je pense que le développement de résolveurs n'a pas eu, on n'a pas travaillé là-dessus pendant de nombreuses années. S'il y avait eu un travail plus structuré au niveau de ces problèmes au niveau de l'industrie. Je pense qu'il y aurait des problèmes qui auraient pu être résolus ou des sauvegardes auraient pu être mises en place pour éviter des problèmes ou pour faciliter la résolution de certains problèmes.

RAM MOHAN: J'encourage d'autres membres du conseil d'administration de poser directement vos questions au lieu de m'utiliser comme intermédiaire.

DAVID CONRAD: Y a-t-il d'autres questions ?

JOHN LEVINE: Oui, est-ce que cela a été mis en œuvre ?

WARREN KUMARI: Je pense qu'il y a… Par exemple Google l'a mis en œuvre. Unbound.

DAVID CONRAD: Très bien, merci beaucoup. S'il n'y a pas d'autre question, alors nous allons passer au point divers sur notre ordre du jour. Est-ce que quelqu'un du groupe d'experts ou du conseil d'administration souhaite que l'on parle d'autre chose ?

YOSHIRO YONEYA: Bonjour, je voulais savoir comment déployer BCP38. Le fait de déployer cela est important pour diminuer les attaques par fausses requêtes. Je pense que Jay a fait un bon travail, en parlant de cela parce que les pratiques opérationnelles doivent être expliquées au niveau de l'IETF, mais il est important aussi que le groupe d'opérateur puisse aussi réfléchir à cette question.

DAVID CONRAD: Le SSAC a publié certains documents par rapport au déploiement de BCP38. On avait dit qu'il est important de réitérer la valeur de BCP38. Mais ce n'est pas un sujet sur lequel le groupe d'experts va se focaliser. Ram, est ce que vous avez quelque chose à ajouter ?

RAM MOHAN: Je vais mettre ma casquette de membre du conseil d'administration, et je voulais fournir des commentaires au groupe d'experts, au TEG.

On a l'impression qu'il y a certains éléments dans notre prochaine itération que l'on devrait considérer pour essayer que ces discussions puissent être un peu plus dynamiques, que ce soit plus un dialogue.

Quand on établit l'ordre du jour, et les sujets que l'on va aborder, on devrait établir une espèce de synthèse simple, qui explique quel est le problème à aborder et pourquoi il nous concerne, ou quelle est l'importance de ce problème. Je pense que c'est ce qui manque ici. Parce que pour nous du côté technique, on lit le sujet, on comprend très bien de quoi on parle, mais si vous n'êtes pas quelqu'un qui vient de la technique, j'ai l'impression que parfois ces sujets que l'on aborde sont parfaits pour qu'une personne qui n'appartient pas à la technique dise : ha non, ça c'est trop technique, je ne veux même pas parler de cela. Et donc voilà.

D'autre part, dans la phase d'élaboration de cet ordre du jour, il serait utile d'inviter les membres du conseil d'administration à nous faire des commentaires, notamment les gens qui ne viennent pas du monde de la technique, pour voir quels seraient les sujets que l'on pourrait aborder, qui peuvent être utiles pour les gens qui ne sont pas de la technique.

Et finalement, je pense qu'il y a le besoin, on voit qu'il y a un certain besoin de mettre en place des séances d'explications,

explicatives, didactiques, pour que ces informations puissent, après, faire partie d'une espèce de référentiel de séances didactiques. Parce qu'il s'agit de sujets importants et les gens de la communauté me disent souvent : nous on fait des politiques, vous, vous faites de la technique là. Et même le niveau technique que nous faisons dans ces réunions est peu accessible pour les gens qui n'appartiennent pas à la technique.

DAVID CONRAD: Merci beaucoup.

WARREN KUMARI: Le but de ces réunions, c'est de connecter le conseil d'administration, les ressources techniques du conseil d'administration. Je pense que nous saluons, bien sûr, les questions qui peuvent nous être posées par le conseil d'administration.

Et en ce qui concerne les séances didactiques, est-ce que le conseil d'administration veut savoir, veut avoir une synthèse par rapport à ce dont on va parler ? Ou bien le conseil d'administration veut des séances didactiques qui expliquent plutôt aux gens de la salle de quoi il s'agit? Pour que les informations soient mieux digérées.

DAVID CONRAD: Il est clair qu'il y a un certain intérêt par rapport à ce type de séances didactiques. Nous avons toute une série de publications intitulées « comment cela fonctionne », qui sont adressées à la communauté et aux nouveaux arrivants. Et nous envisageons la possibilité d'étendre cela à d'autres sujets. Ce serait peut-être l'occasion pour que le conseil d'administration puisse avoir ce type de matériels, de ressources.

En ce qui concerne l'ordre du jour, j'ai essayé de trouver le meilleur moyen d'établir les points de l'ordre du jour que nous allions aborder, en demandant directement aux membres du conseil d'administration, en demandant directement aux membres du TEG, et c'est ce que l'on a pu faire pour cet ordre du jour.

Bien sûr, je souhaiterais avoir d'autres feedbacks pour voir quels sont les sujets qui vous intéresseraient le plus. Cette réunion a notamment pour but de vous donner des informations. Donc nous voulons le faire de la manière la plus appropriée.

Nous allons essayer donc d'obtenir davantage de commentaires.

RAM MOHAN: Oui. J'ai un exemple à vous donner, David. Il y a eu un rapport dans toute la presse il y a quelques semaines, par rapport à une

attaque à l'infrastructure de réseau. Au niveau du conseil d'administration, on se posait des questions non pas au niveau de ce qui avait été informé, mais par rapport à ce que cela veut dire. Comment on pouvait se pencher sur ce type de problèmes.

Donc c'est une question d'interprétation et d'analyse surtout qui semble être nécessaire.

DAVID CONRAD: Warren ?

WARREN KUMARI: Oui, bien sur les membres du conseil d'administration sont très occupés, et prennent deux heures de leur temps aujourd'hui pour quelque chose qui ne leur apporte pas de la valeur. Donc ce n'est pas vraiment très raisonnable. De toute façon, on apprécierait du feedback pour savoir si les sujets sont bien orientés, s'ils sont trop techniques, ce qui serait de votre intérêt, etc.

DAVID CONRAD: Maartenn ?

MAARTEN BOTTERMAN: Oui, j'étais tout innocent au moment de venir, je pensais que c'était une séance qui était liée à ma mission. Et donc au début

je me suis dit : ha, je suis un peu en rapport avec ce qu'ils font, c'est dans la portée de mon travail. Mais si vous êtes sensé informer les autres comme moi, ayons donc des séances didactiques d'une part, parce que les séances pourraient être un peu plus simples si on avait des informations de contexte auparavant. Et puis essayez d'avoir des présentations qui aient un niveau abordable pour les personnes intéressées avec des idées, pour que ce soit bénéfique pour nous tous. Merci de faire ces efforts. Merci.

DAVID CONRAD: Steve ?

STEVE CROCKER: Je suis d'accord avec tous les commentaires concernant les ajustements, mais je voudrais faire un commentaire sur le fait que c'est dans le contexte que cet engagement et cet échange par rapport aux commentaires qui ont été faits, est tout à fait valable.

Cela nous donne un autre niveau d'exposition au sein du conseil d'administration, cela nous permet d'être plus au courant des problèmes techniques qui arrivent. Et c'est très important pour pouvoir générer davantage de sensibilisation par rapport à ces

problèmes, même si on n'est pas en mesure de suivre dans les détails ce qu'il se passe.

Donc je suis très content et je veux m'assurer que ce n'est pas tout simplement une critique ou que des commentaires négatifs qui parviennent à nous. Je pense que le processus qu'on a mis en place ici est très valable et qu'il pourrait évoluer dans la durée, bien sûr. Mais je suis très content de voir que l'on commence déjà à travailler à partir de cette base.

DAVID CONRAD: PatriK?

PATRIK FALSTROM: Merci, je suis membre du TEG de SSAC, et je voudrais vous demander une précision Ram. Vous demandiez une déclaration de problèmes avant la présentation et pas tellement d'avoir une présentation technique.

RAM MOHAN: Oui, exactement Patrik. Ce n'est pas que c'est trop technique, et qu'on devrait être moins technique, mais plutôt qu'il faudrait que l'on commence par savoir pourquoi on soulève cette question, pourquoi elle semble être importante. Et par la suite

d'entrer dans les détails techniques pour avoir un certain contexte.

DAVID CONRAD: Cherine ?

CHERINE CHALABI: J'ai beaucoup profité de cette séance. Surtout pour ce qui est du premier sujet abordé et du dernier sujet qui a été présenté.

Il me semble que du point de vu contextuel, ce sont des présentations fortes utiles, mais ce qui est clair, à mon avis, lorsque vous dites que la réunion du TEG et le board est une réunion conjointe, je pense que ça veut dire que vous allez probablement vous réunir avec un sous-ensemble du conseil d'administration qui arrive à suivre les sujets que vous traitez.

Mais si vous voulez impliquer le conseil d'administration davantage, de façon à ce que tout le monde puisse participer à ce type de rencontres, il faudrait que l'on fasse deux choses. D'une part que soit envoyé du matériel préalable pour préparer les personnes par rapport aux sujets principaux qui seront abordés dans la séance conjointe. Et d'autre part augmenter le niveau de discussions pour que ce soit plus intéressant.

Pour nous, Steve, il faut que l'on s'occupe de savoir clairement quel est le résultat attendu de ce niveau d'interaction. Pour moi, ce n'est pas clair en ce moment. Merci.

STEVE CROCKER: Oui. Concernant la proportion du conseil d'administration qui s'est impliquée à cette réunion, l'approche de base, c'est ma responsabilité d'ailleurs, mais l'approche de base que nous avons adoptée pour interagir avec David était que le groupe de travail d'experts vient pour interagir avec le conseil d'administration. Donc il faut qu'il y ait une certaine interaction avec le conseil d'administration.

Mais d'autre part, comme vous le savez bien, le conseil d'administration a un programme très chargé. On n'a pas demandé formellement à ce que tous les membres du conseil d'administration soient présents.

Donc la situation pratique, et ce que nous avons ici, est qu'il y a une bonne proportion du conseil d'administration représenté ici, et cela correspond à ce que nous essayons de faire, qui est de ne pas demander à tous nos membres de tout faire, mais de nous diviser en comité, en sous-groupe. Donc c'est exactement cette version de facto, ad hoc de cette procédure d'autodésignation, j'ai même invité Göran, qui était là au début. Donc on pourrait, je pense, compter 10 administrateurs de

l'ensemble du conseil d'administration composé par 20 personnes y compris les agents de liaison et le personnel.

Donc c'est vraiment une bonne proportion, c'est nous qui avons choisi de venir participer ici.

Cette autodésignation, de choisir de venir participer ici est positive. Vous voyez.

Je ne me sens pas mal à l'aise par rapport à la portée de ces discussions. Peut-être que d'autres personnes comme vous n'ont pas de connaissances techniques, mais vous comprenez lorsqu'on vous explique.

Il y a d'autres personnes autour de la table qui sont dans la même situation.

On pourrait très bien ajuster le processus, mais je suis content du niveau de participation que nous avons eu et de l'effet que nous avons connu aujourd'hui. Bien sûr, cela peut être peaufiné.

DAVID CONRAD: Warren ?

CHERINE CHALABY: Permettez-moi de répondre. Merci Steve. Je pense qu'il est important de gérer les attentes. Je pense que vous avez expliqué cela clairement.

Je voudrais savoir ce que sent le groupe des experts techniques par rapport à cette interaction à ce niveau avec le conseil d'administration, ce serait intéressant de le savoir.

CHERINE CHALABI: Je sais que vous êtes occupés, mais si vous avez le temps, veuillez nous faire parvenir des retours d'informations à travers Barbara. Par exemple pour savoir comment on peut améliorer ce type de séance, ce qui est utile pour vous, ce qui ne l'est pas, pour que ce soit plus enrichissant dans l'avenir.

CHERINE CHALABY: Retour immédiat, c'était très utile, très enrichissant. Merci.

DAVID CONRAD: On est 8 minutes en retard, mais nous remercions la communauté de la transition IANA dans ce cocktail qui nous attend, pour lequel nous sommes en retard. Donc je vous rappelle qu'on a un cocktail dans la casbah du Westin également. Nous avons deux bus qui nous amènent là-bas qui quitte le centre de convention d'ici 5 minutes ou 7 minutes, je ne sais plus. Et puis une deuxième navette qui quitte le centre de convention à 19 h 15.

Le cocktail à la casbah dans le Westin commence à 19 h 30 et dure jusqu'à 21 h 30 et va servir de l'alcool.

Ok, 19 h et 19 h 30, ce n'est pas ce que dit mon calendrier, mais d'accord, les navettes quittent à 19 h et 19 h 30, donc deux navettes qui partent d'ici à 19 h et 19 h 30.

J'espère vous voir là-bas. Autrement je vais boire toutes les consommations !

[FIN DE LA TRANSCRIPTION]