BARCELONE– DNSSEC pour tous : Un guide pour débutants
Dimanche 21 octobre 2018 – 15h15 à 16h45 CEST
ICANN63 | Barcelone, Espagne

WES HARDAKER : […] la manière dont le DNSSEC fait en sorte que le monde soit plus sûr pour tous. Et on va vous le présenter par l'intermédiaire d'une petite histoire, « Les origines du DNSSEC » qui ont commencé à 5000 avant J.-C., avant même l'avènement de l'Internet.

Et nous allons vous présenter Ugwina qui vit au bord du Grand canyon. Pour ceux qui ne savent pas ce qu'est le Grand Canyon, c'est un trou énorme au milieu des États-Unis. Et ça, c'est Og. Il vit dans une grotte de l'autre côté du Grand canyon. Et ils sont séparés par une longue distance, donc ils n'ont pas beaucoup l'occasion de se parler. Ça prend deux ou trois jours de passer d'un bout à l'autre du Grand canyon.

Et lors d'une de leurs rares visites, ils voient qu'il y a une petite fumée qui vient du feu de Og, et très rapidement, ils utilisent des signaux de fumée pour se parler entre eux, jusqu'à ce qu'un jour, un homme des grottes malicieux apparait. Kaminsky. Kaminsky s'installe à côté de la grotte d'Og et commence à envoyer également des signaux de fumée. Kaminsky, c'est une personne qui a découvert une vulnérabilité très importante du DNS, il y a quelques années.

Donc Ugwina est un peu confuse ; elle ne sait plus quel est le signal de

fumée auquel elle peut faire confiance. Quel est celui qui vient d'Og ? Donc Ugwina va jusqu'à l'autre bout du Grand canyon pour essayer de régler ce problème, et elle va voir le sage du village pour voir s'il a une idée. L'homme des grottes, Diffie, c'est le sage en question ; c'est l'un des inventeurs les plus importants dans le domaine. Donc Diffie s'en va en courant au fond de la grotte et trouve une couleur qui est dans la grotte d'Og, et il en fait une fumée bleue. Maintenant, Ugwina et Og peuvent parler tranquillement en sachant que personne ne va pouvoir interférer dans leurs discussions parce que seulement Og a cette fumée bleue caractéristique.

Donc voilà un petit peu la présentation du DNSSEC avec un diagramme un petit peu simpliste.

Parlons du DNS un peu parce qu'il fonctionne un petit peu de la même manière que ces signaux de fumée. Il y a trois structures dans le DNS, ou une hiérarchie. Et ça commence avec la racine en haut. En dessous, il y a tous les TLD qui comprennent les ccTLDs, les nouveaux TLD, les gTLD. Et en dessous de cela, il y a les points d'enregistrement où les choses se produisent.

Donc je vais vous inviter à garder celui qui est au milieu, bigbbank.com ; on va y revenir par la suite. Donc la racine délègue des informations au serveur com qui envoie des informations à son tour à bigbank.com pour répondre à votre requête, « où se trouve www.bigbank.com » ; elle ne connait pas toute la hiérarchie, mais elle sait où se trouvent le point et la structure pour y arriver. Donc chaque niveau dans cette hiérarchie fait référence au niveau suivant. Donc le

résolveur peut suivre la chaine jusqu'à ce que la réponse soit trouvée, et il cache cette information pour utilisation future et pour que ça prenne moins de temps la prochaine fois, parce qu'il va cacher l'information d'ici la prochaine utilisation.

Mais il y a un problème avec le DNS : il n'a pas été conçu avec quelque type de sécurité tel que les signaux de fumée. Le DNS n'en a pas non plus. Naïvement, on pense que tout est correct. Et il y a des spoofs. Et les caches, s'il y a une mauvaise réponse dans les caches, eh bien, cette mauvaise réponse va se répéter par la suite.

Donc on va vous faire un petit sketch. Combien d'entre vous ont vu ce sketch avant ? Quelques-uns déjà. Alors, pour les autres, ce sera une surprise. Bien. Alors je vais demander à un volontaire de se lever, mes acteurs qui se sont portés volontaires de bien vouloir se lever. Alors nous avons quelques acteurs.

L'utilisateur lambda Joe va être l'utilisateur qui a besoin de faire une opération bancaire en ligne. On a le représentant de la racine de l'arbre DNS, le fournisseur de services Internet, le .com et bigbank.com ; non, en fait, Fred, il vaut mieux que tu te places là.

Donc je vais les laisser parler maintenant. Allez-y. Ça y est. Ça marche.

TIM : Bon, j'ai tout cet argent qu'il faut que je dépose. Il faut que j'aille sur www.bigbank.com pour faire un dépôt d'argent.

NOUVEL INTERVENANT : Bon, je ne sais pas où c'est, donc je vais vérifier pour vous. Je vais demander à la racine. Est-ce que vous savez où se trouve www.bigbank.com?

FRED BAKER : Non je n'ai aucune idée. Toutefois, je vous propose quelque chose ; vous pourriez demander à.com et, .com, peut-être qu'il le saura. Il est à 1.1.1.1.

TIM : Parfait. Je vais les appeler. Alors est-ce que vous savez où se trouve www.bigbank.com?

NOUVEL INTERVENANT : Je suis .com 1.1.1.1. Oui effectivement, je peux vous dire où se trouve bigbank.com, le voici. Bigbank est à 2.2.2. Vous voulez y aller ?

TIM : Oui merci. J'ai besoin de savoir où se trouve www.bigbank.com.

NOUVEL INTERVENANT : Merci, Monsieur FSI. Oui effectivement, je peux vous dire exactement où se trouve www.bigbank.com ; c'est à 2.2.2.3.

TIM : Merci. Bigbank.com est à 2.2.2.3 ! Parfait, je peux aller y faire mon

dépôt d'argent. Merci BigBank.

FRED BAKER : Non. Moi, je crois que c'est lui qui doit vous remercier.

WES HARDAKER : Merci, chers acteurs. Restez parmi nous parce qu'on va avoir besoin de vous d'ici un instant. Oui, en fait, ils font ça à plein temps. Ils sont acteurs à plein temps.

Alors Ugwina, lorsqu'elle tchatte avec Og, ça ressemble un peu au sketch que vous venez de voir. Elle communique avec des signaux de fumée. Il n'y avait pas de problème. Personne n'interférait. Ensuite on va voir ce qui se passe lorsqu'un problème survient. Est-ce que vous pouvez répéter votre petit sketch ?

NOUVEL INTERVENANT : Oh ! j'ai 1 million de dollars qu'il faut que je dépose. Il faut que j'aille sur www.bigbank.com ; je vais aller voir mon fournisseur de services Internet et lui demander comment parvenir à www.bigbank.com !

NOUVEL INTERVENANT : Aucune idée. Je vais demander. Bonjour. Est-ce que vous savez où se trouve www.bigbank.com?

FRED BAKER : Merci. Je suis la racine. Je ne sais pas, mais peut-être que vous pourriez demander à .com, peut-être qu'il le saura. Il est à 1.1.1.1.

TIM : Bien, merci. Bonjour .com, savez-vous où se trouve www.bigbank.com?

NOUVEL INTERVENANT : Oui je suis .com, je vous dirais où il se trouve bigbank.com ; il est à 2.2.2.2.

TIM : Bonjour. Savez-vous où est www.bigbank.com ?

NOUVEL INTERVENANT : Oui, bien sûr, c'est à 6.6.6.6.

TIM : Merci.

NOUVEL INTERVENANT : Voilà www.bigbank.com se trouve à 6.6.6.6.

NOUVEL INTERVENANT : Parfait, je vais aller y faire mon dépôt.

NOUVEL INTERVENANT : Merci.

WES HARDAKER : Bien. Merci à tous. Donc la vraie question, c'est « comment est-ce qu'on va pouvoir se défaire du méchant ».

Donc Ugwina, le résolveur, est confuse ; c'est un peu la situation qu'on vient de voir. Il y a deux signaux. Elle ne sait pas auquel elle peut faire confiance. Et on a tendance à croire la personne en laquelle on croyait auparavant. C'est en tout cas ce qui se passait avant le DNSSEC.

Donc on revient au premier diagramme. Peut-être que vous allez obtenir deux réponses de bigbank.com et vous ne savez pas laquelle est digne de confiance. Mais le DNSSEC ajoute une sécurité au DNS avec des signatures numériques qui ajoutent une couche de sécurité. Ça garantit que l'information n'a pas été modifiée et qu'elle provient du bon endroit. Donc, quelles que soient les caches qui ont été incluses, vous savez d'où vient l'information. Les clés et signatures sont stockées dans le DNS. Donc dans le système de recherche, les clés et les signatures, tout comme toutes les autres données, peuvent être stockées.

Donc le concept de haut niveau du DNSSEC est le suivant. Le résolveur, c'est non seulement où la racine est, mais également la clé racine, et il peut vérifier le reste de l'arbre en constituant une chaine de confiance. Chaque niveau signe le niveau suivant et les données

contenues dans ce niveau jusqu'à ce que la chaine soit complète. Et de cette manière, le résolveur et le fournisseur de services Internet peuvent déterminer quel BigBank est correct, le bleu ou le rouge ; le rouge étant le faux, et le bleu le correct.

Donc, voyons ce qui se produit avec le DNSSEC dans ce petit sketch, et il y a des choses qu'on va évoquer aujourd'hui. Vous voyez ces médailles, ce sont des signatures numériques, et chacun de ces trois serveurs DNS va avoir une médaille. Et ici, on va octroyer une médaille pour être sûr qu'on parle à la bonne personne. Allez-y.

TIM : J'ai un autre dépôt à faire. J'ai besoin d'aller à www.bigbank.com pour faire ce dépôt.

NOUVEL INTERVENANT : Bien sûr, je vais faire la recherche pour vous. Bonjour la racine. Pouvez-vous me dire où se trouve www.bigbank.com?

FRED BAKER : Oui, je suis la racine et je peux vous prouver l'authenticité de ma déclaration. Mais je n'ai aucune idée où se trouve www.bigbank.com. Vaut mieux que vous demandiez à .com et il se trouve à 1.1.1.1.

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

NOUVEL INTERVENANT : Bonjour, je suis .com ; vous pouvez le vérifier. Oui. Vous voyez. Je le suis. Je vais vous dire où se trouve www.bigbank.com : 2.2.2.2.

NOUVEL INTERVENANT : Bonjour BigBank, pouvez-vous me dire où se trouve www.bigbank.com?

NOUVEL INTERVENANT : Oui, bien sûr, mais je n'ai pas de signal donc vous devriez me rejeter.

NOUVEL INTERVENANT : Oh non ! Au revoir. Deux signatures. Bonjour bigbank, pouvez-vous me dire où se trouve www.bigbank.com?

RUSS MUNDY : Oui. Oui, www.bigbank.com se trouve à 2.2.2.3.

TIM : Merci. Est-ce que je peux vérifier votre signature ? Voilà. www.bigbank.com se trouve à 2.2.2.3. Très bien. Je peux aller faire mon dépôt en toute tranquillité. Et voilà.

WES HARDAKER : On va applaudir nos excellents acteurs pour ce dernier petit sketch et

je note qu'il faut qu'il y ait une petite sonnerie quand la signature est reconnue, pour le prochain sketch.

Et c'est ce qui se produit réellement dans le système du DNS et c'est réellement ce qui se produit avec le DNSSEC. Bien sûr, c'est un peu plus complexe que ça, mais dans les faits, les résolveurs ont une chaine à mesure qu'ils avancent. Il y a plusieurs niveaux jusqu'à la réponse finale.

Et donc le DNSSEC protège la chaine jusqu'en bas ; vous obtiendrez une réponse sécurisée. Et tout comme la fumée bleue protège le résolveur pour vérifier que c'est Og qui a envoyé le bon message, le DNSSEC fonctionne de la même manière.

Donc maintenant, je vais passer la parole à Russ Mundy. J'aurais dû d'ailleurs me présenter. Je suis de l'Institut d'information, et Russ Mundy va vous expliquer pourquoi il vous faut utiliser DNSSEC.

RUSS MUNDY : Merci et merci à nos autres acteurs qui nous ont accompagnés aujourd'hui. Ça a été très amusant de le faire avec de nouveaux acteurs parce qu'on avait une nouvelle équipe d'acteurs. Merci aux nouveaux acteurs qui nous ont rejoints.

Alors ça, c'est la séance DNSSEC pour tout le monde. L'objectif, c'est d'aider les gens à réfléchir à la raison pour laquelle quiconque que ce soit, un utilisateur final, un FSI, un opérateur de services, voudrait opérer avec la validation DNSSEC. Et on vous l'a montré avec les

médailles parce que c'est un petit peu la fonction du DNSSEC. Et lorsque vous y pensez, lorsque l'on parle de cela en termes de DNS, ça montre bien que le DNS, ça n'est pas simplement un transfert d'argent. Il y a également des applications qui sont utilisées pour ce faire.

Donc lorsque les gens sont en train d'attaquer le DNS et en train de remplacer des informations, dans la plupart des cas pour ne pas dire tous, il y a d'autres fonctions et applications qui sont utilisées sur l'Internet. Donc si votre DNS ne fonctionne pas correctement, que ce soit le navigateur, le serveur e-mail, une source ou une autre, ça ne va pas fonctionner correctement, et vous ne parviendrez pas là où vous voulez arriver. Donc ça, c'est le problème fondamental et c'est la raison pour laquelle vous voulez que le DNS fonctionne bien, parce qu'il doit bien fonctionner pour que les autres applications que vous utilisez puissent aussi bien fonctionner.

Donc, la grande menace que notre petit sketch entend démontrer, c'est de se concentrer pour faire en sorte que ces logiciels d'application puissent s'adresser à un endroit où l'utilisateur final ne pensait pas arriver. Et parfois, il y a eu un certain nombre d'applications qui ont été attaquées, avec l'attaque qui a commencé au niveau du DNS. Et certaines des attaques ont commencé avec le DNS et ont fini par être une utilisation, ont utilisé trois voire quatre autres protocoles ; mais ça a commencé avec le DNS en obtenant des informations du DNS que les auteurs de cette fraude voulaient utiliser ailleurs et à leur avantage.

Donc je pense que, à un moment donné, il y a eu un cours à l'université. En fait, il y a eu des cours à deux universités différentes où on demandait aux étudiants d'écrire, d'élaborer une attaque DNS, ce qui vous donne une idée de la facilité que cela implique. Mais bon, il n'y a plus ces cours à l'université, mais il y a des informations en ligne. Et ces informations ne touchent absolument pas à l'aspect éthique. Et même si les professeurs demandaient aux étudiants d'élaborer cela dans le cadre de leurs études, l'aspect éthique n'était absolument pas abordé.

Donc cette menace existe. Et pour les gens qui sont intéressés par l'élaboration de logiciels, c'est très important. Donc comme Wes vous l'a dit auparavant, et comme on vous l'a montré avec le petit sketch, quelle est l'idée du DNSSEC ? C'est que les informations cryptographiques présentes dans la structure traditionnelle du DNS, parce que le DNSSEC fait partie du DNS et fait partie du DNS standard, donc lorsque la personne qui reçoit l'information reçoit une réponse signée qu'il y a une validation qui a lieu à un réservoir local, alors l'idée de base est que l'utilisateur qui a envoyé la demande d'information peut obtenir une assurance cryptographique que ces informations proviennent de là où elles doivent provenir et qu'elles n'ont pas été modifiées.

Donc ce que ça fait exactement, c'est que ça vous permet d'être certain que les réponses ou plutôt que les informations que vous devriez utiliser, que vous utilisiez des serveurs mail et que ceux-ci parlent l'un l'autre, que ces informations sont dignes de confiance. Donc vous voyez ici deux exemples simplifiés sur cet échange. Vous

voyez l'utilisateur Joe qui fait sa demande. Je n'ai pas modifié les chiffres utilisés sur les T-shirts des acteurs. Donc requête de Joe auprès de son fournisseur de services Internet, le serveur récursif qui ensuite envoie la demande pour parvenir à l'endroit où Joe veut aller. Il obtient une réponse de la part du serveur faisant autorité et du serveur récursif. Ça, c'est le premier scénario avec le petit sketch.

Le suivant. Ah attendez. Après que la réponse arrive, en fait, c'est un flux entre les applications elles-mêmes. Donc l'utilisateur Joe parle ensuite au serveur Web et fait son activité là.

Maintenant lorsque vous avez une série de zones signées DNSSEC, vous pouvez concevoir des sites Web avec des indications pour démontrer que la bonne information est échangée. Et dans la plupart des cas, la grande majorité des sites Web n'ont pas d'indicateur de ce type. Mais c'est quelque chose qu'on a fait il y a quelques années pour que les gens puissent facilement voir qu'ils obtenaient une chaine DNSSEC dans ce flux d'informations. Et si vous n'aviez pas d'authentification DNSSEC, alors vous obteniez une information différente.

Donc dans la conception des sites Web, on a introduit un indicateur d'attaque. Et cet indicateur, c'est un petit peu la même chose que le méchant du sketch où une information est envoyée au serveur faisant autorité. Mais avant même que le serveur faisant autorité intervienne, le méchant intervient et donne une fausse information. Donc l'utilisateur Joe va sur le mauvais site, celui du méchant. Entre-temps, la requête est envoyée au DNS et envoyée sur le réseau, mais

l'utilisateur Joe et sa machine ont d'ores et déjà obtenu une réponse, donc ils ignorent la bonne réponse et envoient la demande pour se connecter au site du méchant, et n'obtiennent jamais cette information jusqu'à ce que le DNSSEC intervienne.

Lorsque le DNSSEC intervient, l'utilisateur Joe rejette la mauvaise réponse que vous avez vue sur ce petit sketch et va sur le bon site. Et dans ce cas-ci, ce site Web a les bonnes informations. Et même si on l'a fait sur le même site Web, on l'a conçu de telle manière que cela illustre qu'on va sur deux sites Web différents. Donc ça, c'est ce qu'obtiendrait un bon serveur de validation avec une petite coche verte, mais un résolveur non validé, vous le voyez ici. Steve Crocker disait, par exemple, que l'ICANN ne résoudra pas le problème de la faim dans le monde. Donc la même chose pour les FSI.

Donc les informations ont été insérées sur le site Web de telle sorte que les utilisateurs n'auraient aucune idée du fait que le site Web aurait fait l'objet d'une attaque substantielle du DNS. Vous pourriez donc dire qu'il n'y a pas beaucoup de résolution du DNS. Non.

En fait, comme vous le voyez à l'écran, nous avions mesuré CNN il y a 10 ans. Voilà maintenant sur l'écran, il y a cinq ans. Donc une page de contenu de cnn.com a fait l'effet de tant de demandes DNS. Donc il y a eu beaucoup de demandes. Donc l'information sur le DNS et le DNSSEC est donc la partie critique dans la zone des données.

Voilà une autre illustration qui démontre les processus et leur fonctionnement. Ça vous démontre aussi où les changements

devraient avoir lieu. Comme vous voyez sur la gauche, il y a la zone d'informations qui va vers le serveur d'autorisation. Il y a aussi le serveur récursif qui répond aux questions qu'on lui aura posées, que le client lui aura posées. Si le client pose la question comme vous le voyez sur la première flèche en bleu, il y a la deuxième démarche, la troisième démarche qui va vers le serveur récursif, et ensuite vous avez la réponse du serveur récursif vers le client.

Donc lorsque vous mettez en œuvre le DNSSEC, il y a des étapes que vous devez suivre dans lesquelles vous avez des fonctionnalités additionnelles. Donc, la mise en œuvre, pour votre partie du DNS, la partie dont vous êtes responsables, que vous devez opérer ou gérer, eh bien cela dépend d'où vous vous trouvez dans la structure de DNS. Les activités qui sont vraiment intégrées dans le DNS vont devoir faire tout cela par eux-mêmes. Donc si la complexité et la taille de ce que vous faites est vraiment bien mise en place par rapport au DNS, comme vous le voyez à l'écran, vous voyez, il y a des exemples lorsqu'il y a donc beaucoup d'activités et quand il s'agit de zones qui ne sont pas critiques, disons, mais qui sont faciles à gérer, voilà, ces gens-là vont peut-être mettre les choses en place par eux-mêmes.

Donc, encore une fois, protéger la zone est un facteur critique.

Donc voilà sur la dernière illustration, vous voyez que l'information, la protection de la zone doit être rajoutée. Il faut que ce soit simple. Il faut qu'il y ait donc une information qui soit signée et qui soit ancrée dans le système par la personne qui possède le serveur d'authentification d'autorité. Il faut qu'il y ait processus de validation

vis-à-vis du serveur récursif qui donc lui-même va valider encore une fois, et qui va dire « oui, oui, oui, voilà tout cela est correct au niveau cryptographique » à l'organisation existante avec laquelle vous travaillez, par exemple, ayant beaucoup d'activités, beaucoup de fonctionnalités. Et là, vous allez pouvoir le faire de façon interne. Si cette activité a une utilisation délimitée au niveau du DNS et il y a une des chances qu'il y a un département IT ou qu'il y a façon de sous-contracter une tierce partie pour le faire,

Pour les fournisseurs, que c'est le département externe ou interne, et qui peuvent donc mettre en place DNSSEC, et s'ils ne peuvent pas le faire. Il faut qu'ils apprennent parce que sinon vous allez aller faire affaire avec une tierce personne et il y a beaucoup de personnes qui peuvent le faire. Il y a beaucoup d'organisations qui vont choisir une tierce partie pour faire ce travail d'implémentation du DNSSEC.

Voilà donc, c'est la fin de la présentation principale et nous allons pouvoir maintenant voir si l'audience a des questions.

Je vais passer la parole à Wes parce que nous avons beaucoup d'acteurs DNSSEC dans cette salle. Mais nous avons aussi beaucoup de personnes qui sont compétentes dans le sujet du DNSSEC. Posez donc les questions sur les thèmes qui vous intéressent et on vous répondra.

WES HARDAKER : Le DNSSEC – oui. J'ai des problèmes de micro. Bon très bien. Nous avons maintenant deux micros.

Le DNSSEC n'est pas simple. C'est un système complexe. Et nous sommes surs qu'il y aura des questions à ce sujet donc nous avons laissé une bonne portion de temps pour pouvoir répondre à vos questions. Il y a des experts dans cette salle qui ont aidé à la création du DNSSEC. Donc si vous avez des questions, on peut vraiment y répondre. Si vous avez des questions, encore une fois, levez la main. Nous vous apportons un micro volant.

THANH NGUYEN : Bonjour, je suis du Vietnam. Je vous remercie de votre présentation qui est très utile. Nous avons pris beaucoup d'informations sur la sécurité du DNS. Je vois qu'il y a beaucoup d'apprentis du DNSSEC lorsqu'il s'agit de déployer pour sécuriser les ccTLD ou les gTLD, mais quand on parle de la mise en application du DNSSEC, est-ce qu'on doit parler des défis auxquels on va faire face ?

Et là où il s'agit de la signature de la zone, il y a d'autres étapes que j'ai oublié. Mais si je me base sur ces étapes, on peut subir des attaques DDoS ? Et il faut synchroniser au niveau temporel parce que cela prend du temps pour mettre tout cela en place. Vous avez vu. Nous avons vu ça sur vos diapositives. Cela prend donc beaucoup de temps au niveau de la réponse. Est-ce que vous pourrez faire les choses plus rapidement avec le système DNSSEC. Est-ce que vous avez des solutions pour résoudre ce problème ?

WES HARDAKER : Oui ; vous posez deux-trois questions, là. Tout d'abord, vous avez

demandé s'il y avait un délai plus long pour les utilisateurs afin qu'ils demandent les autorisations. Donc tout cela ralentit un petit peu le processus. Toutes ces étapes ralentissent le processus un petit peu. Mais les utilisateurs qui utilisent des applications instantanées sont ceux qui sont les plus concernés. Ils doivent regarder toutes les réponses et, typiquement, ce n'est pas facile.

À cause des caches, il va y avoir un ralenti pour les recherches. Même les données de sécurité seront sous les caches. Donc ce sera d'une milliseconde plus lent, mais en général, il y a vraiment un délai. Ce délai sera observé une fois par une des FSI.

Donc vous posez aussi la question au sujet des données, de la base de données du DNS, car elles sont très importantes. Donc il y a, si vous avez une question au niveau des réponses de retour, si vous falsifiez la direction à laquelle vous allez, à ce moment-là, vous allez vous adresser à la mauvaise personne.

Il y a aujourd'hui des limites au niveau des réponses, et ce sont des limites qui sont soutenues par la plupart des serveurs, surtout quand il y a des demandes de beaucoup de données en même temps. Et si vous ne faites pas la chose correctement, on va vous dire non on ne peut pas vous répondre.

En fait, je suis responsable moi-même d'un des serveurs racine. Et avec nos retours instantanés, nous obtenons beaucoup de demandes comme ça. Et cela se passe souvent. Mais bon, c'est en problème qui a eu lieu il y a des années ; maintenant ça va.

Warren, vous voulez parler ? Non ? Vous voulez vous asseoir avec nous ? S'il y a des experts dans la salle, ils peuvent nous rejoindre sur la scène.

EBERHARD BLOCHER : Eberhard Blocher, je viens d'Allemagne, je ne suis pas un expert. Je suis vraiment un personnage lambda.

J'ai une question. Dans le passé, je sais que le DNSSEC existait déjà. Je pense que ça a commencé il y a une dizaine d'années avec Steve Crocker. Donc si je comprends bien, nous avons eu donc beaucoup de temps depuis le début du DNSSEC, et nous avons encore des questions. Moi je fais du DNS pour certains de mes clients. Nous avons du cryptage qui est gratuit et c'est une manière de sécuriser les sites Web. Et je comprends que c'est aussi typique d'avoir un lien vis-à-vis d'un seul nom de domaine.

Donc la question est : est-ce qu'on a encore besoin du DNSSEC ? Quelle est la différence entre le DNSSEC et les sites Web cryptés ? Si j'encrypte mes sites Web, j'ai un certificat, donc pourquoi aurais-je encore besoin du DNSSEC ?

Pour la deuxième question, j'ai regardé les statistiques, et je sais que beaucoup d'opérateurs de registre fournissent des données et, vous savez, il y a des bureaux d'enregistrement qui ont très peu de pénétration. Quelle en est la raison ? Et c'est la même question. C'est la même réponse. Est-ce qu'on a besoin du DNSSEC ?

WES HARDAKER : Très bonne question. Donc une des choses les plus importantes au niveau de la sécurité en général de l'Internet, on ne peut pas résoudre un seul problème, parce que tout fonctionne en couches, si vous voulez. Donc si par exemple vous faites une recherche DNS, disons que vous allez sur un site qui est protégé. Vous savez que vous êtes au bon endroit sur le bon site Web, si vous y arrivez. Le DNS rentre en jeu bien avant ça. Et pourquoi ? Vous pouvez vous diriger sur le mauvais endroit. Il y a des soucis. Vous pouvez aller au mauvais endroit dès le début et ne jamais atteindre le bon site Web.

Donc il y a la protection du routing. Donc comme vous le savez, l'Internet est construit en couches. Donc chaque couche doit être protégée. Donc que le DNSSEC est toujours utile et nécessaire.

Vous avez des informations à nous donner sur ce qui s'est passé il y a 10 ans avec Steve Crocker. D'ailleurs, je crois que Steve l'a vraiment aidé.

RUSS MUNDY : Oui, il y a un historique important au niveau du DNSSEC, dans la conception du DNSSEC, la mise en application et le déploiement du DNSSEC. Ceci a pour but de nous assurer que l'utilisation du DNS obtient la bonne réponse pour l'utilisateur. Et cela se passe de façon indépendante. Mais en fait, c'était en 1993 que nous nous sommes concentrés. Nous avons concentré nos efforts sur le développement du DNSSEC et sur sa conception. Il y avait eu beaucoup d'appels aller-

retour. D'ailleurs Steve Crocker était vraiment très présent durant ces conversations et j'en faisais partie aussi de cette conversation. Il y a eu beaucoup de conceptions qui ont été refaites et refaites parce que c'était quelque chose qui était fait très rapidement pour pouvoir sécuriser les protocoles en cours.

Il y avait deux conceptions qui avaient des problèmes. Donc la troisième conception était la bonne, en 2010. C'est là que la zone racine a été signée.

Oui bien sûr, il y a eu beaucoup de personnes qui ont beaucoup contribué. Il y a beaucoup d'organisations qui ont travaillé très dur sur le sujet. Mais comme on l'a dit tout à l'heure, la focalisation s'est mise sur qui se passe là, sur l'écran. Que vous utilisiez un certificat SSL ou pas, il y a toujours des défis avec les autorités qui publient les certificats. Il peut y avoir de mauvais certificats et on n'est pas sûr d'avoir les bons résultats. Et on peut avoir un CA problématique sur le site Web, et ainsi, l'utilisateur va toujours obtenir un site signé SSL.

WES HARDAKER : Oui, la toile n'est pas le seul système qui doive être protégé. Il y a des choses qui ne peuvent pas être résolues avec les certificats. Je vais en parler, d'ailleurs, mercredi durant l'atelier de travail du DNSSEC. On en parlera tout à l'heure. Tout le monde peut venir. Et là, on parlera plus en détail du DNSSEC. Le DNSSEC, est-ce que c'est la seule solution disponible pour protéger le DNS ou les humains ? Donc un certificat typique SSL ne peut pas faire la même chose que le DNSSEC.

AHMAD ALSADEH : Pourquoi est-ce que tout le monde ne déploie pas le DNSSEC ? C'était ma première question.

Est-ce que vous croyez aussi que les nouvelles technologies pourraient représenter des solutions prometteuses dans le domaine ?

WES HARDAKER : Alors, oui. On nous a demandé pourquoi certains opérateurs de registres ont déployé et pas d'autres. Oui, c'est une très bonne question.

Chaque région dans le monde a un taux de déploiement différent. Certains TLD, surtout en Suède et en République tchèque et dans d'autres pays d'ailleurs, ont donné des incentives financiers pour que vous signiez la zone. Souvent, il s'agit d'incentives qui sont plus importants ou s'il y a vraiment un effort local pour pousser les compagnies et les entreprises à utiliser cette technologie.

En fait, nous avons maintenant des statistiques numériques. Il y a des millions de zones qui ont été signées même si les pourcentages sont bas puisqu'il y a des milliers de millions de noms. Nous en sommes à 85 % des TLD qui ont signé à ce jour. Donc on arrive, mais c'est un processus très long pour que tout le monde, le monde entier, y participe.

RUSS MUNDY : Oui, il y a une autre raison ; ce n'est pas seulement les TLD et les domaines de deuxième niveau, mais les utilisateurs finaux n'ont pas forcément été très actifs dans leur demande du DNSSEC. La plupart du temps, ils ne réalisent pas l'importance du DNSSEC pour leur fonctionnalité, pour le fonctionnement. Mais durant les cinq dernières années, le gouvernement américain a donc mis en place des exigences pour que tous les .gov soient signés. Et certains autres gouvernements ont suivi cet exemple. Moi je connais le problème des États-Unis. Je suis plus familier avec ce sujet-là. Mais ils ont demandé qu'une validation soit faite pour tous les domaines. Donc ça a été repoussé vis-à-vis de beaucoup d'entreprises et d'organisations. Par exemple, la compagnie avec laquelle je travaille, parsons.com, est un domaine signé et opère de cette manière.

Donc il faut continuer à éduquer, à encourager les gens dans leur demande du DNSSEC. Demandez à vos FSI ou à vos fournisseurs tout simplement pour savoir s'ils ont ce service DNSSEC.

WES HARDAKER : Oui, beaucoup de bureaux d'enregistrement et d'opérateurs de registres ont juste à pousser un bouton. C'est assez facile. Mais beaucoup de personnes qui ont leur propre DNS, cela coute de l'argent. D'ailleurs, c'est le cas pour tous les mécanismes de sécurité, que ce soit le DNSSEC ou autre ; il faut se former sur le sujet et en apprendre plus.

Il y a des outils maintenant qui rendent les choses plus faciles, mais il y

a 10 ans, c'était compliqué.

Y a-t-il d'autres questions ?

INTERVENANT NON IDENTIFIÉ : Bonjour. Ma question est au sujet des problèmes de la signature de la clé de la semaine dernière.

Est-ce qu'il y a des plans pour ajouter ça pour pouvoir détecter ça au niveau des noms de domaine ?

WES HARDAKER : Le roulement de clé de la semaine dernière était le premier. Ça s'est passé très très bien d'ailleurs. Est-ce que vous voulez en parler, John ?

Alors le roulement donc s'est très bien passé. Il y a eu certaines FSI qui ont été impactées. Ils ont dû changer leur clé. Mais de façon générale, ce sont les FSI qui ont besoin de cette clé. Comme vous l'avez vu tout à l'heure, l'utilisateur Joe n'a pas dû faire grand-chose. Il ne savait même pas que le DNSSEC est intervenu dans la chaine. Donc c'est un autre problème.

Mais bon de façon générale, seulement les FSI ont besoin de savoir ce qui se passe niveau du roulement de la clé.

Pour l'ICANN, nous allons voir si cela se produira encore à l'avenir. Nous allons discuter durant cette réunion. D'ici une année, on va voir combien de fois on va le faire, quel va être le mécanisme qu'on va suivre pour faire le roulement de cette clé. Donc c'est quelque chose

que nous allons déterminer après ce qui s'est passé la semaine dernière.

RUSS MUNDY : Oui, la communauté aura vraiment — va participer sur la décision de la date du prochain roulement de clé. C'est quelque chose que l'ICANN et les organisations veulent vraiment faire. Il nous faut des informations de retour, des contributions de la communauté. Il faut partager ces informations. Il y a des mécanismes qui sont mis en place pour obtenir toutes ces informations de la part de la communauté.

WES HARDAKER : Il y aura encore une fois une présentation mercredi sur le roulement de clé durant l'atelier de travail du DNS.

JOHN LEVINE : J'ai une question ; vous savez, j'ai toujours des questions. J'héberge le DNS pour beaucoup d'utilisateurs. Donc pour la moitié de ces zones, je suis le bureau d'enregistrement. Donc j'ai accès à toutes les données, et j'ai accès donc aux signatures du DNSSEC. Pour les autres, je suis une tierce partie. Pour tous les utilisateurs, vous savez, les seuls qui peuvent faire fonctionner le DNSSEC, ce sont les titulaires de noms de domaine. Moi je dois donc former mes utilisateurs sur les processus d'installation du DNSSEC. C'est facile pour vous. Pour moi. Mais ce n'est pas si facile pour tout le monde. Il faut aussi que chacun, que tous les comptes de bureaux d'enregistrement soient accrédités. C'est

quelque chose qu'on peut résoudre au niveau du bureau d'enregistrement pour peut-être trouver une personne qui serait le contact idéal pour ce genre de situation.

Et il n'y a pas vraiment de progrès. Je sais que je ne suis pas un cas commun. Mais je suis sûr qu'il faut absolument régler ce problème,

WES HARDAKER : Oui. Il y a du travail à faire, surtout pour les personnes qui gèrent leur propre zone. Moi je fais ça manuellement. Je sais qu'il y a un effort qui doit être fait. Les choses sont améliorées, surtout durant les deux dernières années. Il y a certains fournisseurs qui créent un bouton, si vous voulez, que si vous publiez, vous pouvez juste cliquer sur une clé ; vous allez juste avoir donc à cliquer sur le bouton.

Et puis il y a aussi un système qui s'appelle CDS pour pouvoir mettre à jour la clé entre la zone et le DNS. Il y a des discussions sur toutes ces choses qui sont en cours, surtout durant le mois dernier. Je voudrais bien en parler, d'ailleurs. Beaucoup de personnes parlent de ce sujet donc on veut maintenant savoir qui a mis en application ça et ça. Je voudrais que Warren nous en parle.

Alors tout d'abord—

INTERVENANT NON IDENTIFIÉ : Oui vous savez, il y a beaucoup de pays qui font ça, comme en République tchèque, en Suisse, au Liechtenstein. Si vous avez une marque sur votre zone, ça l'arrange, les choses sont plus faciles. Au

moins il y a des tentatives dans ce sens. C'est le début. On va beaucoup en apprendre de ce qui s'est passé la semaine dernière. Je pense que quand il s'agit de l'atelier du DNS qu'on va avoir cette semaine, ça va être très utile.

WES HARDAKER : Oui, il y a du travail à faire. Mais bon, je pense que là, on avance bien.

Il y a aussi un panel qui discutera de tout cela mercredi.

RUDOLPH DANIEL : Je suis un boursier à l'ICANN. Je ne sais pas si c'est approprié de parler de ceci ici, mais le roulement de clé, de KSK, qui vient d'être mentionné, jusqu'à présent ça a été réussi. Mais qu'est-ce qui en est sorti ?

WES HARDAKER : Oui. Ça a été un succès jusqu'à présent. Mais les TTL sur les données étaient de deux jours dans le cache. Et puis là, ça fait 10 jours qu'on a fait le roulement. Oui je pense 10 jours. Donc après 10 jours, encore une fois, il n'y a pas eu de résolveur DNS qui aurait dû attendre si longtemps. Ils auraient dû faire la mise à jour des informations. Et maintenant on devrait savoir s'il y a eu un échec ; ce n'est pas le cas. Tout le monde aurait vu qu'il y a eu un échec.

Donc il y a deux aspects. Tout d'abord, nous avons toujours l'ancienne clé dans la zone racine, mais elle n'est pas utilisée. Elle est là, mais elle

n'est pas utilisée. Et le 11 janvier, il y aura un changement drastique qui dira « voilà, c'est le moment de ne plus faire confiance à cette clé ». Et ce sera publié pour trois mois de plus. Et donc, le 11 avril, cela sera retiré de la zone racine.

Donc il y a beaucoup plus d'informations sur le roulement et sur le processus, mais je pense que jusqu'à présent il s'agit d'un succès. Bonne question.

INTERVENANT NON IDENTIFIÉ : Quand il s'agit de l'intégration de l'utilisateur au niveau du moteur de recherche, alors autre question. Je voudrais proposer à mes clients d'utiliser .com, et pas des TLD génériques parce qu'il n'y a pas de signature à ce niveau. Il s'agit de faire de la prévention de marketing et pour aller plus rapidement. Est-ce que vous avez en place des plans pour les utilisateurs pour démontrer que le site auquel ils ont eu accès est le bon site ? Par exemple dans les moteurs de recherche comme [inaudible], etc. Est-ce qu'il y aura une manière de voir si la signature est correcte, et adéquate ?

C'était sur la diapositive tout à l'heure ; j'ai vu qu'il y avait une vérification de la signature. Peut-être que cela devrait être intégré par exemple dans Chrome.

Est-ce quelque chose en vue ? Est-ce que vous avez quelque chose en vue ?

WES HARDAKER : Oui. Il y a donc une extension pour les moteurs de recherche qui s'appelle DNSSEC. Je ne me rappelle plus du reste. Je sais que c'est bon pour Firefox et pour Chrome. Il y en a un qui est installé dans votre moteur de recherche. Les vendeurs dont de moteur de recherche ne sont pas très intéressés à mettre le DNSSEC directement sur le site. Il faut prendre contact avec eux, communiquer avec eux, et se plaindre.

Alors, ça s'appelle DNSSEC-Validator ; vous pouvez l'installer. Et d'ailleurs, il y a des années, nous avons travaillé sur un moteur de recherche qui avait donc intégré le DNSSEC.

RUSS MUNDY : Oui. On doit aller voir les informations.

WES HARDAKER : Oui, ça modifiait Firefox pour qu'ils aillent faire directement le DNSSEC, directement avec le moteur de recherche. Il se passe d'autres choses au niveau des e-mails. On en parlera mercredi. Vous verrez, on vous montrera des diagrammes et des informations là-dessus.

BARRY LEIBA : Pour pouvoir parler aux utilisateurs, on doit utiliser les évidences et les preuves qu'on a collectées durant les années passées. Il faut essayer de faire comprendre à l'utilisateur qui ne connait pas de DNSSEC ; ce n'est pas facile.

WES HARDAKER : Oui. En fait, la façon dont on veut mettre en place le DNSSEC, maintenant, c'est juste d'éviter qu'ils arrivent à atteindre ce message. Et là, en général, les gens n'ont pas les connaissances pour prendre une bonne décision qui soit sure.

INTERVENANT NON IDENTIFIÉ : Pour faire un commentaire là-dessus, ça ne veut pas dire que l'on doit s'engager et expliquer à l'utilisateur final pourquoi ce message apparait sur l'écran. Est-ce que ça va — comment est-ce qu'on pourrait faire. Il va y avoir donc des explications à donner. Si c'est la première fois qu'ils obtiennent ce message, c'est bien. C'est nouveau. Mais si le message est bien expliqué, cela pourrait être une bonne manière d'expliquer les choses, car la prochaine fois qu'ils auront ce message, ils comprendront.

WES HARDAKER : Oui, c'est un débat très compliqué et très long pour savoir exactement quelle information on doit partager avec l'utilisateur. Moi j'aime bien avoir des informations très détaillées, mais j'en parle avec des gens que je connais qui ne comprennent pas non plus toutes ces choses-là.

Quelqu'un d'autre a une autre question ?

INTERVENANT NON IDENTIFIÉ : Oui, il y a beaucoup de problèmes par rapport à l'hébergeur local. Par exemple, si vous voyez une notification. Je ne sais pas si vous utilisez un proxy ou autre [inaudible] pour avoir des avantages pour la

signature, mais c'est très important de pouvoir identifier l'utilisateur et d'avoir beaucoup de choses stockées.

WES HARDAKER : Oui, aujourd'hui on parle des noms. Mais si les FSI et le résolveur utilisent l'identification, s'il y a différentes couches, différents niveaux et dans les mails et autres, tous ces chercheurs DNS doivent être validés.

Je crois qu'il y a une personne au fond. C'est toujours derrière vous pour les questions.

JOSE ALBERTO : Bonjour, c'est Jose Alberto ; je suis boursier, donc je fais partie du programme des boursiers de l'ICANN. Ma question est liée à Tor.

Nous utilisons Tor, par exemple, pour le DNS appliqué à Tor. Et dans ce cas-là, je ne sais pas s'il serait possible d'utiliser un nom autre type de DNS sécurisé.

WES HARDAKER : Oui effectivement. Ça me rappelle que je n'ai pas répondu à la question sur le block-chain qui m'a été posée auparavant. Alors, il y a plusieurs systèmes de noms. Il y a le Tor un, il y a un chercheur de noms également, qui ne sont pas compatibles avec le DNS. Le DNSSEC protège uniquement le DNS, ce qui n'empêche pas d'utiliser les autres mécanismes, ce qui n'empêche pas d'avoir son propre système de

sécurité. Mais je ne pense pas que le DNS s'applique à Tor. Peut-être que théoriquement oui, ça pourrait s'appliquer. Mais malheureusement, je ne suis pas expert en Tor. Donc je ne sais pas comment répondre, mais j'aurais tendance à répondre que non. Mais il faudrait que vous voyiez quelqu'un qui s'y connaisse mieux en Tor. Je ne suis pas expert moi-même, ça ne marchera pas. Bon. Voilà. La réponse définitive, ça ne marchera pas.

FAN-CHIEH LIN : Bonjour. Je suis Jason, une fois encore. Alors je crois comprendre que le DNSSEC est conçu pour protéger les transactions DNS. Et j'ai lu un article qui disait que les cookies DNS introduits par [RFC MT3 MP4] sont censés être une méthode plus légère pour résoudre cela.

Est-ce que vous pourriez développer cet argument et j'espère que je ne m'éloigne pas du sujet qui nous occupe maintenant.

WES HARDAKER : Non. Les cookies DNS permettent de résoudre un problème tout à fait différent, et d'ailleurs la première phrase que vous avez dit, il y avait une petite erreur. Ça n'est pas faux , mais vous avez dit que c'est pour protéger les transactions. Non, le DNS ce n'est pas pour protéger les transactions, mais les données.

Laissez-moi vous donner un exemple. Si je devais donner à Russ des informations DNS et je lui dis mon nom d'hébergement, c'est 1.1.1 ; et il peut donner cette information à toute la salle. Ça permet de fermer

toutes les données, quelle que soit la manière dont on transporte ces données, ces informations. Ça n'est pas la connexion qui est protégée par le DNSSEC, c'est la donnée elle-même. Et ça, c'est important en raison du cache, parce qu'avec le DNS, vous pouvez utiliser des hubs multiples parfois.

Si vous d'utiliser les résolveurs Google 8.8.8, vous pouvez utiliser des caches. Et quelle que soit la personne qui répond et qui pose la question, peu importe la manière dont vous avez obtenu une réponse. Le mécanisme des cookies a été conçu pour protéger une transaction unique contre des choses qui sont parfois trop grandes et qui vous permettent d'avoir une réponse plus grande que ceux à quoi le serveur peut répondre. Donc c'est un problème différent que traitent les cookies. Le DNSSEC ne protège pas les données à l'intérieur des transactions DNS.

INTERVENANT NON IDENTIFIÉ : Pour sécuriser les données DNS, on a deux mécanismes différents. D'abord le DNSSEC et ensuite INS par rapport au TLS qui joue un rôle de sécurité. Donc je vous vois que le DNSSEC est plus populaire que le TLS, est-ce que vous pouvez développer un petit peu quelle est la principale caractéristique du DNSSEC par rapport à l'autre ?

WES HARDAKER : Oui, les objectifs sont différents aussi. Le DNSSEC là encore a pour objectif de protéger les données. Donc, que ce soit avec le TLS ou pas, quelle que soit la manière dont vous avez obtenu les informations,

tandis que le TLS est conçu pour protéger les transactions entre une personne qui pose une question et là où ils obtiennent la réponse. Ce que vous ne savez pas, c'est si votre moteur de recherche demande à votre FSI pour vous assurer que personne ne voit votre requête. Mais personne ne peut demander au FSI de demander aux résolveurs par l'intermédiaire de TLS.

Donc le DNSSEC protège l'intégrité et permet de savoir si vous avez la bonne réponse, tandis que le TLS protège la confidentialité des données pour être sûr que personne ne voit votre requête et la réponse que vous retenez. Peut-être que le TLS sera un jour utilisé partout, mais maintenant parce qu'il y a plusieurs « hops » entre le point A, B, C, D pour s'assurer que c'est sécurisé, le DNSSEC permet de sécuriser cela quel que soit le nombre de « hop ».

KEN HERMAN : Ken Herman, consultant indépendant. Donc oui, vous avez parlé du niveau de pénétration. Combien de gens l'utilisent ? Comment est-ce que les organisations, les individus peuvent savoir que le DNSSEC a mis en place cette chaine de confiance. Et troisièmement, pouvez-vous nous en dire un peu plus par rapport au cout que ça représente pour que les organisations mettent en œuvre ? Peut-être que ce n'est pas beaucoup pour une petite organisation, mais pour les grandes organisations, qu'en est-il ?

WES HARDAKER : Alors, venez à l'atelier du DNSSEC mercredi avec des informations.

D'ailleurs cette semaine, c'est mercredi. C'est plus tard dans la semaine que d'habitude. Parce qu'on va vous donner beaucoup de données d'information par rapport à la pénétration, dans quelle partie du monde on l'utilise le plus, y compris une présentation sur les noms de domaine.

[L'interprète s'excuse. Il y a des coupures de micro].

Donc, venez s'il vous plaît.

Quelle était la deuxième partie de la question, s'il vous plaît. Oui les couts.

Avant c'était beaucoup plus difficile de le faire. Si vous me demandiez d'allumer la validation DNSSEC, peut-être que les gens ne l'auraient pas fait avant qu'on leur demande. Donc c'est plus une question qui a à voir avec le fait qu'aujourd'hui il y a très peu de configurations pour l'activer. Donc il y a très peu d'excuses. Ils ont besoin de savoir ce qui se passe lorsqu'il y a un roulement de clé. Aujourd'hui, c'est beaucoup plus évident. Au début, il fallait signer une zone. Si vous alliez le faire vous-même, signer vous-même, alors, il y avait une série de douze commandes.

D'ailleurs, on a élaboré un guide précoce, à l'époque. Et un de nos collègues a trouvé un outil avec un espace unique pour le faire. Donc, les outils sont beaucoup plus simples. Donc le cout est moindre, mais il y a toujours l'aspect sécurité.

Autre chose importante à savoir. Avant il s'agissait de publier/oublier ;

vous publiez une chose et vous l'oubliez pendant trois ans. Avec le DNSSEC, parce que ça implique de dédier du temps, moi je resigne ma zone toutes les deux semaines par exemple.

INTERVENANT NON IDENTIFIÉ : Une remarque par rapport à ce que vous venez dire. Comme vous le savez, avec les résolveurs et les enregistrements CDS, vous les publiez une fois, et ensuite il y a un mécanisme automatique qui se charge de tout cela. Donc les couts sont minimes.

WES HARDAKER : Oui effectivement ; excellente information que vous donnez. Avec les résolveurs faisant autorité, les résolveurs automatiques, il y a toute une série de choses qui sont faites de manière automatique.

Y a-t-il d'autres questions dans la salle ? D'ailleurs excellente question, toutes les questions qui ont été posées jusqu'à présent.

THANH NGUYEN : J'ai une autre question qui n'est pas technique : pour certains pays comme le Vietnam, puisque je viens du Vietnam, pour le gouvernement, le système DNS—

Par exemple, pour nous, le système DNS n'est pas sûr. Et on veut passer au DNSSEC pour tout le système DNS. Donc quel serait le cout pour ce transfert au DNSSEC, et quels seraient la durée que vous pourriez estimer et les couts que vous pourriez estimer ?

WES HARDAKER : C'est difficile à estimer tout ça. Je ne suis pas bien sûr de la réponse.

RUSS MUNDY : J'aimerais faire quelques commentaires. Je ne vais pas vous donner de réponse précise, mais je peux vous donner une idée. L'une des choses qui a été identifiée par les gens lorsqu'ils ont commencé à faire du DNSSEC et à faire fonctionner le DNSSEC, c'est qu'ils ont souvent découvert que le logiciel DNS n'avait pas été correctement mis à jour. Donc peut-être qu'ils l'utilisaient sur leur serveur faisant autorité ou s'ils opèrent également les FSI et utilisent des serveurs récursifs, qu'ils utilisent des versions qui datent d'il y a cinq ou 10 ans. Donc il faut voir l'état de votre structure DNS. Si elle est bonne, cette structure, et à jour comme on l'a dit auparavant, la difficulté ou plutôt le défi qui se pose dans l'utilisation du DNSSEC peut être aussi simple que le fait de changer deux ou trois paramètres dans le dossier de paramétrage pour ce qui est de la distribution au serveur faisant autorité. Et ça peut être beaucoup plus compliqué si vous voulez mettre en place un mécanisme crypté séparé.

Mais la chose la plus importante et la première chose à faire c'est de voir la structure du DNS lui-même et, à partir de là, il y a toute une série d'informations disponibles en ligne. Et la communauté DNSSEC a été incroyablement utile pour partager au fil du temps cette information. Il y a des tonnes d'informations disponibles en ligne pour documenter ce qui se passe dans chaque pays.

WES HARDAKER : Donc l'ISOC. D'ailleurs le site Web que vous avez vu au départ avec la photo de Steve Crocker, c'est un excellent site pour commencer, vous orienter et voir comment avancer. C'est un site Web très utile qui a beaucoup d'information. Il y en a un qui s'appelle DNSSEC-Tools. Il y en a un autre qui est un peu plus « geeky ».

Et ensuite les couts, ça dépend de ce que vous voulez faire. Et comme disait Russ, il a commencé par vous dire il faut voir ce que vous faites actuellement pour voir d'où vous démarrez, pour voir ce que vous voulez faire après.

RUDOLPH DANIEL : Rudy au micro, boursier ICANN. Oui. Je me rappelais de quelque chose qu'on appelle EDNSSEC. Est-ce que ça vous dit quelque chose ?

WES HARDAKER : EDNS, sans le SEC, EDNS tout seul. C'est une extension dans le mécanisme DNS pour ajouter des informations supplémentaires lorsque vous faites une requête d'informations. Et c'est là que vous dîtes, je veux faire du DNSSEC ; donnez-moi toutes les signatures et toutes les choses. Donc c'est un mécanisme d'extension du DNS, dont le DNSSEC a besoin.

Dernière question peut-être dans la salle ?

BARRY LEIBA : Si vous avez une minute, j'aimerais revenir sur ma première question par rapport au DNSSEC et le HTTPS.

À l'origine, il n'était pas nécessaire d'aller sur un site Web pour avoir accès aux HTTPS. Vous étiez redirigé. Donc on n'utilisait pas le HTTPS. Donc vous aviez besoin d'une vérification. Et ensuite, on a eu besoin d'un transport sécurisé et on nous disait d'utiliser toujours le HTTPS, et ils n'acceptaient jamais une connexion sans HTTPS. Ça, c'était pour intercepter toutes menaces à la première requête. Maintenant, il y a une liste de transport sécurisé stricte, et on vous dit n'essayez jamais d'avoir accès à ce site Web en particulier. Et comme l'a dit Russ, si vous regardez votre moteur de recherche, vous voyez toutes les autorités des signatures avec VeriSign et une entreprise dont vous n'auriez jamais entendu parler de Taiwan.

Et là, si vous cherchez un certificat pour bigbank.com, là, vous avez un problème. Avec une banque qui donne ses propres informations comme Dane par exemple, ça, ça peut résoudre un problème. Mais il faut voir quelle est la requête de Dane ; quelle est la requête de Dane DNSSEC parce que vous obtenez un certificat de la part du DNSSEC. Et ça revient à ce que disait Russ, tout est en couches et il faut protéger tout.

WES HARDAKER : Et la réalité veut que la première chose que les utilisateurs mettent, ce soit un nom. Ce nom est recherché. Et ça, c'est le premier point de vulnérabilité. Donc, la manière de contourner tous ces problèmes,

c'est cela. Mais si vous avez un système de sécurité, il y a tous ces problèmes qui se posent.

Et après, si vous utilisez HTTPS, ça règle toute une série de problèmes.

Y a-t-il peut-être une dernière question dans la salle ?

AHMAD ALSADEH : Ahmad Alsadah au micro, boursier ICANN.

Alors, lorsque j'ai vu votre sketch, je me suis rendu compte que tout le monde sur la chaine doit avoir un certificat, une signature. Si l'un n'est pas déployé, alors le DNSSEC ne fonctionne pas. C'est bien ça ? J'ai bien compris ?

WES HARDAKER : Oui presque. Ce n'est pas qu'il y a un échec. Mais vous savez définitivement que vous allez à un endroit qui n'a pas été signé par le DNSSEC. Donc il n'y a pas de confiance. Donc il y a des parties de l'arbre DNS qui n'ont pas été signées, parce que le DNS vous donne une partie de la réponse en vous disant vous n'avez que cette partie de l'arbre n'a pas déployé le DNSSEC. Donc les résolveurs avancent sur la chaine et ils vous disent, voilà, à partir de là, je ne peux pas garantir la sécurité. Voilà où on en est aujourd'hui. Il y a beaucoup de choses qui ont été signées et beaucoup d'autres qui ne l'ont pas encore été.

Et donc il y a une question de visibilité des utilisateurs aussi.

Peut-être que s'il y a une dernière question dans la salle, on a le temps de l'écouter. Oui. Ici.

INTERVENANT NON IDENTIFIÉ : [Micro, s'il vous plait ; les interprètes n'ont pas entendu la question].

Est-ce que vous pouvez obtenir des messages, des messages proches ?

WES HARDAKER : Alors en fait, vous n'obtiendrez pas de messages proches que vous ayez une réponse claire ou pas. À l'heure actuelle, on ne regarde pas ce genre d'information parce que comment présenter cela aux utilisateurs et savoir si c'est une bonne chose, de présenter ou pas aux utilisateurs. Savoir si c'est utile pour l'utilisateur final ou pas, c'est un autre des pas. Ce que vous verrez, c'est qu'il y a un échec du DNSSEC. Dès qu'il y a un méchant qui intervient, alors vous verrez que ce site Web ne va pas être trouvé par exemple, parce que si on essaie de trouver le nom et on continue de recevoir de mauvaises réponses, alors vous obtiendrez la même réponse que pour un site Web introuvable, en disant je ne trouve pas ce site Web. Donc échec de recherche du nom pour vous.

Sur ce, je pense qu'on va s'en tenir là.

Russ, est-ce que vous avez un dernier mot à dire ?

RUSS MUNDY : Oui, nous avons eu un peu de pub dans la salle pour notre réunion de

mercredi. On va parler de Dane. On va parler des cartes qui sont créées pour choisir le niveau et type de déploiement de DNSSEC dans le monde, et représenté de manière géographique. Donc j'invite tout le monde à revenir mercredi. On va commencer à 9 heures et jusqu'à 14 h 30. C'est ça Cathy ? Non. 15 heures. 15 heures. Donc, réfléchissez-y.

Merci à tous d'être venus. Nous espérons avoir répondu à vos questions, mais si vous voulez venir nous voir ici, ou l'un des acteurs qui ont participé au petit sketch si vous avez des questions sur le DNSSEC, nous serons tout à fait ravis d'y répondre. Que ce soit ici ou dans les couloirs. Merci.

WES HARDAKER : Demain, journée Tech. Il y aura également beaucoup de discussions. Je ne me rappelle plus bien de l'agenda, mais en général, il y a des présentations sur le déploiement des TLD dans le DNS, etc.

Oui. À 10 h 30, juste après la cérémonie d'inauguration. Merci à tous. J'espère que vous en aurez bien profité. Merci.

[FIN DE LA TRANSCRIPTION]