COPENHAGUE – Réunion conjointe du Conseil d'administration de l'ICANN et du Groupe d'experts techniques (TEG)
Mercredi 15 mars 2017 – 17 h à 18 h 30 CET
ICANN58 | Copenhague, Danemark

STEVE CONTE : Si quelqu'un cherche le groupe sur l'acceptation universelle, la session a lieu dans la salle B5.1. Ce n'est pas que nous ne voulons pas de vous mais si vous cherchez la session sur l'acceptation universelle au lieu de celle du TEG, c'est dans la salle B5.1 que ça se passe. C'est malin, j'ai envie de jouer à la bataille navale maintenant.

DAVID CONRAD : Quoi ? Ah d'accord. La fête peut commencer. Jonne est là.

>> (hors micro)

DAVID CONRAD : Nous jonglons un peu niveau logistique pour le moment. Steve et Lousewies ont dit être en chemin, donc ils ne devraient pas tarder. Nous essayons aussi de préparer les diapos.

>> (hors micro)

DAVID CONRAD : On peut commencer par les présentations, si vous le voulez bien. Pour info, cette session oppose le Conseil d'administration aux experts techniques dans un match en cage. Bien. Ou pas.

C'est la réunion je ne sais plus combien du groupe d'experts techniques. Cette session a été organisée pour permettre aux experts techniques de donner des informations au Conseil d'administration. Nous n'adressons pas de recommandations, nous donnons juste des faits. Au départ, ce devait être une session à huis clos mais nous avons décidé de la rendre publique pour accueillir tous ceux qui aiment les trucs de geek.

Voyons voir. Quelqu'un a apparemment demandé si le RSSAC et le SSAC étaient invités à cette session. Alors, (a) c'est une réunion ouverte et (b) je pense qu'il y a confusion parce que – C'était à quelle réunion ? Celle de Marrakech ? – je ne sais pas plus à quelle réunion c'était mais on a dû improviser parce

qu'on a dû annuler le TEG pour travailler sur la transition. Donc au lieu d'avoir la réunion du TEG, nous avons décidé d'organiser un cocktail pour le TEG et le Conseil d'administration, et pour rendre la chose un peu plus divertissante, on a aussi invité le RSSAC et le SSAC au cocktail, qui est devenu une sorte de tradition. Les membres du TEG et du Conseil d'administration seront donc les bienvenus au cocktail qui aura lieu ce soir au Ruby vers 19 h.

>> À 19 h.

DAVID CONRAD : À 19 h, sachant qu'il y a un bus qui part à 18 h 45 de...

En fait, vous avez un micro.

>>. Donc, après cette session, à 18 h 45, nous avons une navette assez grande au Bella Center, entrée ouest, juste de l'autre côté en partant d'ici.

Donc à 18 h 45, n'hésitez pas, rejoignez-nous et montez à bord. Merci.

DAVID CONRAD : Steve est arrivé, de même que Jonne, la fête peut commencer.

>> (hors micro)

DAVID CONRAD : Exactement. Tu veux dire quelque chose ?

STEVE CROCKER : Avec joie. Excusez mon retard. Je suis vraiment ravi de voir autant de gens ici. C'est génial. David est aux commandes.

[Rires]

DAVID CONRAD : Bien. Commençons par les présentations.

Marc, si tu veux bien. Donne ton nom, pour qui tu travailles, ta couleur préférée, ce que tu veux, je n'en sais rien.

MARC BLANCHET : Marc Blanchet.

JAY DALEY : Jay Daley, .NZ.

DANIEL DARDAILLER : Daniel Dardailler, W3C.

LITO IBARRA : Lito Ibarra, Conseil d'administration de l'ICANN.

KAVEH RANJBAR : Kaveh Ranjbar, expert technique et membre du Conseil d'administration de l'ICANN.

LARS JOHAN-LIMAN : Lars Johan-Liman, responsables des opérations de serveur racine chez Netnod.

GEORGE SADOWSKY : George Sadowsky, Conseil d'administration de l'ICANN.

RINALIA ABDUL RAHIM : Rinalia Abdul Rahim, Conseil d'administration de l'ICANN.

PATRIK FÄLTSTRÖM : Patrik Fältström, président du SSAC.

ASHWIN RANGAN : Ashwin Rangan, personnel de l'ICANN.

CHERINE CHALABY : Cherine Chalaby, Conseil d'administration de l'ICANN.

MARKUS KUMMER : Markus Kummer, Conseil d'administration de l'ICANN.

TERRY MANDERSON : Terry Manderson, personnel de l'ICANN, directeur du génie DNS et directeur de service au sein de l'IETF pour le domaine Internet.

ALAIN DURAND : Alain Durand, personnel de l'ICANN et chercheur à l'OCTO.

ASHA HEMRAJANI : Asha Hemrajani, Conseil d'administration de l'ICANN.

PAUL VIXIE : Paul Vixie, Farsight Security, invité.

JEREMY RAND : Jeremy Rand, du projet Namecoin.

PAUL WOUTERS : Paul Wouters, agent de liaison de l'IETF.

STEVE CROCKER : Steve Crocker, Conseil d'administration de l'ICANN.

DAVID CONRAD : David Conrad, ICANN.

STEVE CONTE : Steve Conte, personnel de l'ICANN.

CATHY PETERSON : Cathy Peterson, personnel de l'ICANN.

WENDY PROFIT : Wendy Profit, personnel de l'ICANN.

JONNE SOININEN : Jonne Soininen, agent de liaison de l'IETF auprès du Conseil d'administration de l'ICANN.

DAN YORK : Dan York, de l'Internet Society, et je travaille plus spécifiquement sur les DNSSEC.

SUZANNE WOOLF : Suzanne Woolf, SSAC, RSSAC, trouble-fête occasionnel.

WARREN KUMARI : Warren Kumari, agent de liaison de l'IETF.

ED LEWIS : Ed Lewis, ICANN, chercheur à l'OCTO.

ROY ARENDS : Roy Arends, ICANN, chercheur à l'OCTO.

MATT LARSON : Matt Larson, également de l'ICANN et chercheur à l'OCTO.

FRANCISCO DA SILVA : Francisco da Silva, de l'ETSI – l'entreprise pour laquelle je travaille est internationale – Suède.

HOWARD BENN : Howard Benn, également de l'ETSI.

JULIE HAMMER : Julie Hammer, SSAC.

ROD RASMUSSEN : Rod Rasmussen, SSAC.

>> (nom inaudible) de l'ITU-T.

ADIEL AKPLOGAN : Adiel Akplogan, personnel de l'ICANN, engagement technique.

GREG AARON : Greg Aaron, SSAC.

MAARTEN BOTTERMAN : Maarten Botterman, Conseil d'administration de l'ICANN.

JAAP AKKERHUIS : Jaap Akkerhuis, du groupe SSAC/RSSAC.

LOUSEWIES VAN DER LAAN : Désolée du retard. Lousewies Van der Laan, Conseil d'administration de l'ICANN.

JOHN CRAIN : Je me cachais dans le fond et je me suis dit que je devrais venir devant. John Crain, ICANN, directeur de la sécurité, la stabilité et la résilience.

DAVID CONRAD : Bien. Merci beaucoup.

L'ordre du jour est affiché à l'écran. Il s'agit de la session d'accueil et d'administration triviale.

Je répète ce qui a été dit plus tôt : si vous cherchez la réunion du groupe directeur sur l'acceptation universelle, elle a lieu dans la salle B5.1, un peu plus loin dans le couloir. Mais vous êtes les bienvenus ici aussi. Il s'agit bien entendu du match en cage du groupe d'experts techniques contre le Conseil d'administration.

On avance. Je pense que nous allons commencer par la présentation de Jeremy Rand, qui va nous parler du projet Namecoin. Jeremy, si tu veux bien.

JEREMY RAND : Bonjour. Je m'appelle Jeremy Rand, de Namecoin. Allons-y.

Je vais d'abord vous expliquer ce que je fais. Je suis l'un des développeurs les plus actifs de Namecoin et je ne connais aucun développeur de Namecoin qui ne soit pas d'accord avec ça. Mais

bon, je ne peux pas parler au nom de tous les développeurs sur tous les sujets. Nous gérons un projet à code source ouvert qui n'a pas de structure organisationnelle bien définie, sachez-le.

J'ai préparé cette présentation en collaboration avec Hugo Landau.

Namecoin a été créé en partant du principe que les humains se comportent de façon non déterministe et que par extension, tout système géré par des humains se comportera de façon non déterministe.

Plus particulièrement, même si un système est régi par des règles supposément inviolables, des règles établies par des humains ne seront pas toujours strictement respectées.

Par exemple, la Constitution américaine a établi des règles selon lesquelles la torture et la surveillance de masse sont prohibées. Malheureusement, ces règles sont mises en œuvre par des humains et par conséquent, comme nous le savons tous, elles sont loin d'être appliquées aussi strictement que nous le souhaiterions.

Le comportement humain dans un avenir lointain est encore moins prévisible.

Par exemple, plus la date d'une élection est éloignée dans le temps, plus il est difficile d'en prévoir le résultat. De la même manière, le climat politique dans un pays est plus difficile à prévoir à long terme.

Le DNS est en grande partie géré par des humains, ce qui entraîne un risque parce que les personnes chargées de gérer le DNS peuvent se comporter de façon non déterministe.

Votre bureau d'enregistrement peut faire une erreur ou quelqu'un peut modifier vos enregistrements. Peut-être que le gouvernement qui possède votre ccTLD sera renversé dans 10 ans et que le nouveau gouvernement n'aimera pas votre nom et décidera de le saisir. Peut-être que sous l'effet de pressions politiques à l'avenir, l'ICANN appliquera une nouvelle politique avec laquelle vous n'êtes pas d'accord à l'heure actuelle.

Tout cela peut arriver et c'est inquiétant.

Namecoin est une expérience que nous menons pour savoir s'il est possible de concevoir quelque chose de vaguement similaire au DNS, mais avec une contribution humaine minime, afin de créer un système de type DNS qui se comporte de façon plus déterministe que le DNS actuel. Nous espérons qu'un tel système sera plus fiable et mieux protégé des erreurs d'origine humaine, car plus prévisible.

Comparons certains des systèmes d'identificateurs qui existent à Namecoin.

Les systèmes de nommage manuel sur un site, comme les fichiers *hosts*, n'ont pas d'espace de noms mondial, ce qui veut dire que les noms ne sont pertinents qu'au niveau local, mais ils sont à l'abri de tierces parties humaines imprévisibles et ils ont une signification humaine, ce qui est une bonne chose.

Les systèmes de nommage hiérarchique comme le DNS ont un espace de noms mondial mais celui-ci est exposé aux éventuelles erreurs de tierces parties humaines imprévisibles. Ces noms ont une signification humaine. Ce type d'outil est donc facile à utiliser mais risqué en tant que racine de confiance.

Les systèmes d'adressage de contenus comme BitTorrent, où les noms sont hachés, ont un espace de noms mondial à l'abri de tierces parties humaines imprévisibles, mais les noms n'ont aucune signification humaine et les contenus ne peuvent pas être modifiés.

La clé publique est une variante des noms. Comme dans les domaines .ONION utilisés par Tor. Ces systèmes comprennent un espace de noms mondial et sont à l'abri de tierces parties humaines imprévisibles, mais là encore, les noms n'ont pas de signification humaine. Par contre, les contenus peuvent être

modifiés. Ce type de système est sûr comme racine de confiance mais pas facile à utiliser. L'utilisateur voit un URL comme celui que vous voyez à l'écran lorsqu'il essaye de taper quelque chose.

Ce que je dis n'est pas totalement vrai. Tor fait une mise à jour de sécurité pour l'instant mais quand il aura fini, les noms ressembleront vraiment à ça.

[Rires]

JEREMY RAND : Vous avez peut-être remarqué que dans les précédentes diapos, il y avait deux marques et un X, c'est le triangle de Zooko. Zooko Wilco a émis l'hypothèse qu'il est impossible de réunir ces trois propriétés en même temps.

J'ouvre une parenthèse. Les journaux publics *append-only* sont de plus en plus populaires pour garantir la responsabilité. L'exemple le plus parlant est le certificat de transparence de Google. Chaque certificat utilisé sur le web est placé dans un journal *append-only*. Les navigateurs finiront probablement par exiger l'enregistrement de certificats. Même si vous voulez garder le contrôle d'un système, vous pouvez vouloir publier toutes les actions réalisées.

Le certificat de transparence est un journal *append-only* qui répertorie les certificats, mais il n'est pas adapté à des systèmes comme le DNS. La raison à cela, c'est que n'importe qui peut ajouter quelque chose au journal. Mais seuls les certificats émanant d'autorités de certification peuvent être rédigés. C'est bien pour éviter que les journaux soient encombrés de données indésirables, mais établir une liste d'entités fiables est un peu fastidieux.

Namecoin est un journal *append-only* pour les enregistrements de noms et les mises à jour. Mais contrairement aux certificats de transparence, Namecoin fonctionne avec une chaîne de blocs. Il peut donc éviter les données indésirables en imposant un coût pour pouvoir rédiger du contenu. Ce coût est peu élevé mais efficace, et cela dissuade des entités malveillantes de squatter massivement les noms; sans avoir à vérifier une liste des entités fiables.

Namecoin comprend un espace de noms mondial, à l'abri de tierces parties humaines imprévisibles, et les noms ont une signification humaine. C'est donc une solution au triangle de Zooko. Namecoin prouve qu'un journal *append-only* pour le nommage peut être géré comme un forum ouvert, ce qui accroît son utilité. La responsabilité et la transparence peuvent alors devenir des biens publics vérifiables d'un point de vue

cryptographique. Indépendamment du système de règles que Namecoin utilise pour ses noms, sa nature de journal *append-only* signifie que lorsqu'une entité malveillante fait quelque chose, ça se sait.

Comme exercice de réflexion, imaginez une zone racine responsable. La responsabilité peut rassurer des parties méfiantes en garantissant qu'il n'y a rien de louche.

Prenons un exemple hypothétique. Gérer la zone racine comme un journal *append-only* permettrait de prouver aux pays à travers le monde que le contrôle des États-Unis est bien effectif, y compris au niveau intergouvernemental.

Les serveurs racine pourraient se servir directement du journal. Une zone racine gérée comme un journal *append-only* pourrait rassurer les pays qui craignent, par exemple, que leur ccTLD soit compromis pour des raisons politiques, de la même manière que les pays se surveillent les uns les autres en vertu du Traité d'interdiction complète des essais nucléaires, ce qui garantit la paix. Faire confiance, tout en contrôlant ce qui se passe. Soyons clair, je ne recommande pas la mise en œuvre de cette idée dans le DNS, mais c'est une hypothèse intéressante.

Dans un autre domaine, l'un des problèmes liés est l'infrastructure de gestion des clés publiques TLS. Le système

d'autorité de certification utilisé actuellement pose problème, même avec les certificats de transparence. Le problème sous-jacent, c'est qu'il implique trop d'humains imprévisibles susceptibles de faire des erreurs. Les DNSSEC et la DANE, qui enregistrent les données TLS dans le DNS, au lieu d'avoir des autorités de certification pour les vérifier, pourraient améliorer la situation. Malheureusement, là encore, il faut tenir compte de certaines considérations politiques. Certains craignent des abus de la part de la racine DNS ou des opérateurs de TLD.

Une fois de plus, le souci, c'est que la racine DNS et les opérateurs de TLD impliquent des humains. Donc ça ne règle pas complètement le problème de la présence humaine. Namecoin pourrait offrir les avantages des DNSSEC et de la DANE dans ce but, sans les inconvénients politiques.

Nous ne nous attendons pas à ce que la majorité des logiciels ou des services de résolution de noms aient directement connaissance de Namecoin. Nous espérons plutôt qu'un logiciel passerelle entre Namecoin et le DNS sera installé au niveau local, ce qui permettrait de transformer les requêtes DNS en requêtes Namecoin, et les réponses Namecoin en réponses DNS.

Namecoin utilise le TLD .BIT, qui n'est pas enregistré pour l'heure auprès de l'ICANN ou de l'IETF. Nous aimerions trouver un moyen simple d'arranger ça. Nous avons conscience que

c'est un problème. Par exemple, nous pourrions utiliser le registre de noms à usage spécial, comme .ONION pour Tor.

Notre service de limitation, appelé NCDNS, fonctionne comme un serveur DNS fiable pour le TLD .BIT, qui fonctionne sur le localhost. Les utilisateurs de DNSSEC génèrent un temps d'installation, et nous faisons en sorte que la spécification des noms de domaine de Namecoin reste facile à cartographier pour le DNS, ce qui facilite l'utilisation d'un logiciel passerelle.

Dans l'hypothèse où vous voudriez vous en servir, vous pourriez dire à votre serveur DNS récursif, par exemple Unbound, d'utiliser NCDNS pour .BIT et lui fournir la clé publique DNSSEC de NCDNS. En théorie, tout ça devrait marcher. Et ça ne représente que quelques lignes sur unbound.net.

Dans la pratique, certaines caractéristiques du DNS ne sont pas soutenues par beaucoup de systèmes. C'est le cas de la DANE pour la TLS. Nous devons donc réaliser des exercices de multiplication spécifiques bizarres pour faire fonctionner tout ça. Une fois, j'ai essayé de compter les différentes couches d'actions réalisées pour faire fonctionner la DANE de Namecoin sur les navigateurs qui ne supportent pas la DANE pour la TLS. Je me suis arrêté à cinq.

Dans quelles situations réelles le comportement déterministe de Namecoin peut nous aider ? Admettons que vous essayez d'acheter ou de vendre un nom. Dans le DNS, acheter ou vendre un nom implique généralement un risque de contrepartie, et vous pouvez être amené à faire appel à intermédiaire pour limiter ce risque.

Dans Namecoin, l'acheteur et le vendeur peuvent convenir d'une transaction atomique à l'issue de laquelle le vendeur est payé et le nom transféré à l'acheteur. Cela élimine le risque de contrepartie sans avoir à faire appel à un intermédiaire.

C'est super mais si le vendeur et l'acheteur ne veulent même pas se parler pour convenir de la transaction atomique ? Vous pouvez acheter ou vendre des offres. Ça fonctionne comme ça : Alice peut créer une offre de vente. « Je vends le nom de domaine exemple.bit pour 100 namecoins. » Alice signe l'offre de vente avec sa clé privée, ce qui prouve qu'elle possède exemple.bit et qu'elle est prête à le transférer moyennant 100 namecoins. Alice peut publier cette offre de vente signée sur un forum ou ailleurs.

Bob voit l'offre et veut acheter exemple.bit. Il répond à l'offre en signant avec une clé privée sur laquelle il y a 100 namecoins. Cette offre est devenue une transaction Namecoin valide. Bob

peut ensuite aller sur le réseau Namecoin sans avoir à contacter Alice.

Alice est payée. Bob reçoit le domaine. La transaction est atomique. Il n'y a aucun risque de contrepartie et il n'est pas nécessaire de faire appel à un intermédiaire. Ça marche aussi bien pour les offres d'achat que de vente. Le protocole Namecoin supporte déjà ce type d'actions, et nous espérons pouvoir bientôt proposer des outils faciles aux utilisateurs.

Prenons un autre exemple. Un nom appartient à une clé privée unique mais il peut aussi appartenir à plusieurs clés privées, auquel cas les clés M-de-N doivent être présentées pour faire une mise à jour. Ce peut être une protection efficace si une clé unique est compromise. Par exemple, les membres d'un conseil d'administration peuvent chacun avoir une clé privée, mais mettre à jour le nom peut exiger la majorité qualifiée du conseil. Là encore, le protocole Namecoin supporte ce type d'actions et nous espérons pouvoir bientôt proposer des outils faciles aux utilisateurs.

Namecoin permet aussi des politiques de mise à jour très flexibles, qui peuvent servir à personnaliser certaines choses en fonction de la sécurité ou des besoins UX d'un titulaire de nom. Par exemple, admettons qu'Alice possède un nom mais qu'elle souhaite limiter le risque qu'on lui vole sa clé privée, sans

accroître le risque de contrepartie. Elle peut très bien concevoir une politique du genre : Alice peut contacter Trent pour gérer un service d'authentification à deux facteurs. Alice peut ensuite mettre son nom à jour avec des données arbitraires, si Trent signe ses mises à jour. Et Trent s'engage à signer uniquement après avoir procédé à une vérification grâce à une authentification à deux facteurs.

Mais en plus, Trent peut signer à l'avance des transactions spécifiques pour certains événements, au cas où Alice voudrait faire quelque chose par la suite sans l'approbation de Trent. Par exemple, peut-être qu'Alice veut pouvoir annuler son enregistrement TLSA pour pouvoir révoquer le certificat facilement si jamais son serveur web est compromis. Ou peut-être qu'Alice craint que Trent ne disparaisse, arrête son activité ou perde sa clé privée. Ces politiques peuvent être rédigées selon les besoins propres de chacun. Trent ne peut pas transférer ou mettre à jour le nom d'Alice sans la signature de cette dernière, et Alice peut vérifier si les transactions signées à l'avance sont valides et si elle est protégée de Trent avant d'appliquer cette politique à son nom. Ces politiques sont rédigées dans un langage spécifique et appliquées au même niveau que les signatures courantes.

Namecoin ne signe pas l'arrêt des bureaux d'enregistrement. Dans Namecoin, ils ressembleraient beaucoup à Trent. Mais Namecoin limite davantage que le DNS le risque que les bureaux d'enregistrement nuisent à leurs clients, de façon accidentelle ou malveillante. Peut-être que ça poussera les bureaux d'enregistrement à réduire leur budget sécurité.

Les services comme ceux de Trent n'existent pas encore dans Namecoin, mais j'aimerais bien que ça devienne une réalité. Prenons un autre exemple. L'infrastructure du DNS a récemment été la cible d'attaques par DDOS, comme celle contre Brian Krebs. Certains ont avancé que Namecoin pourrait être un outil de défense utile. Je ne vois pas trop comment Namecoin pourrait résister à une attaque DDOS.

Mais je sais que le réseau Bitcoin a été soumis à des exercices de simulation de crises, qui ressemblent aux tentatives d'attaque DOS qui ont eu lieu ces dernières années. Ces exercices ont été effectués par des entreprises à but lucratif qui avaient un intérêt financier à essayer de donner l'impression que le réseau Bitcoin ne peut pas résister à ce genre d'attaques. Mais Bitcoin n'a pas franchement été affecté. Est-ce que Namecoin s'en sortirait aussi bien ? Est-ce que les attaquants auraient les mêmes ressources que les entreprises qui ont réalisé les exercices de simulation de crises sur Bitcoin ? Difficile à dire. Mais je pense

vraiment que c'est un cas intéressant. J'aimerais voir plus de recherches à ce sujet à l'avenir.

Afin de parvenir à ce déterminisme, il faut quand même faire des compromis. Ainsi, les transactions Namecoin sont irréversibles. Par conséquent, lorsqu'un nom est transféré à un nouveau titulaire, l'ancien titulaire ne peut pas le récupérer sans la signature du nouveau titulaire. Ça veut dire que les noms Namecoin sont plus susceptibles de faire l'objet d'une reprise hostile par des programmes malveillants. Dans la même veine, toute erreur commise par le titulaire du nom peut aussi poser problème.

Une solution éventuelle consisterait à garder vos clés privées sur une machine protégée par un *air gap* ou peut-être d'attribuer des politiques de signatures multiples ou d'authentification à deux facteurs. Mais ce n'est pas si mal. J'ai entendu des experts en sécurité dire que l'un des plus gros avantages publics de la popularité de Bitcoin était que les gens prenaient enfin au sérieux la sécurité des terminaux. Au fur et à mesure que Bitcoin se développe, je pense que la sécurité des terminaux ira en s'améliorant. Donc ce sera peut-être moins un problème à l'avenir.

Autre compromis, dans Namecoin, il n'y a pas d'humains imprévisibles chargés de déterminer quels enregistrements de

noms sont valides. C'est pour ça que ce système a des avantages en matière de sécurité et qu'il est moins susceptible d'être affecté par des considérations politiques. Mais ça veut dire que lorsque quelqu'un enregistre un nom qui empiète sur une marque déposée, il n'existe pas de moyen simple d'annuler cet enregistrement. Il faut négocier avec la personne qui a procédé à l'enregistrement.

C'est plutôt inhérent à la définition d'atteinte aux marques. Déterminer s'il y a atteinte nécessite une intervention humaine, et Namecoin est explicitement conçu pour ne pas être géré par des humains.

Une solution éventuelle serait d'amener les utilisateurs à consulter une liste de noms portant atteinte à des marques déposées bloqués quelque part entre le client Namecoin et le navigateur web de l'utilisateur. Par exemple, le logiciel DNS utilisé comme passerelle entre Namecoin et les applications DNS pourrait supporter cette option. Il existe déjà des infrastructures pour des choses dans ce genre, comme PhishTank.

Le souci, c'est qu'un utilisateur qui souhaite voir un nom qui porte atteinte à une marque déposée pourrait volontairement désactiver le blocage. Mais puisque l'objectif du droit des marques est d'éviter la confusion pour les consommateurs, ce

n'est peut-être pas un si gros problème. Un utilisateur qui fait ça sait probablement ce qu'il fait. On pourrait aussi avancer que quelqu'un pourrait acheter un nom qui porte atteinte à une marque déposée dans le seul but de le vendre au propriétaire légitime de la marque. Mais étant donné que l'enregistrement des noms a un coût, il est difficile pour une seule personne de squatter un nombre important de noms de la sorte, de la même manière que le coût des noms du DNS limite le risque de squattage.

Un autre compromis concerne la vie privée. Étant donné que l'ensemble des transactions réalisées via Namecoin est public, tout le monde peut consulter ces informations. L'analyse du graphique des transactions permet assez facilement de savoir si deux transactions ont été réalisées par la même personne. Le problème se pose aussi pour Bitcoin. Ça veut dire que si vous enregistrez deux noms Namecoin à des fins différentes, il apparaîtra publiquement que les deux ont été enregistrés par la même personne.

Si vous achetez des namecoins à quelqu'un, la personne pourra voir les noms enregistrés avec. Une solution consisterait à acheter des namecoins grâce à un moyen de paiement qui ne laisse pas de trace en public. Ce qui signifie que vous ne devriez pas utiliser des bitcoins pour acheter des namecoins si vous

tenez au respect de votre vie privée. Vous devriez également utiliser des paires de clés publiques et privées séparées pour chaque nom que vous achetez pour éviter qu'on fasse le lien dans le graphique de transaction. Les virements bancaires peuvent être un moyen d'acheter des namecoins sans laisser de trace en public. En plus, des essais ont été réalisés pour créer des monnaies de type bitcoin plus respectueuses de la vie privée, comme Monero et Zcash, que vous pouvez utiliser pour acheter des namecoins, puis des noms. Ces systèmes présentent leurs propres inconvénients mais ils peuvent en valoir la peine pour certains utilisateurs.

En règle générale, la référence de mise en œuvre de Namecoin respecte assez peu la vie privée et ne permet pas franchement d'empêcher le public d'apprendre que vos noms ont le même titulaire. Nous voulons apporter des améliorations dans ce domaine parce que c'est un vrai problème.

Le dernier compromis concerne la sécurité de la nature *append-only* de Namecoin. Toutes les propriétés de sécurité de Namecoin sont vérifiables d'un point de vue cryptographique, à une grosse exception près, c'est que la protection du classement des opérations relatives aux noms Namecoin n'est pas sûre d'un point de vue cryptographique. Elle n'est sûre qu'en termes économiques, ce qui signifie que reclasser ces opérations

coûterait beaucoup d'argent. Et plus vous remontez dans le temps, plus ça coûte cher. Namecoin part généralement du principe que le classement ne bouge probablement pas pendant deux heures maximum après la réalisation d'une opération relative aux noms. Mais ce n'est pas protégé d'un point de vue cryptographique. C'est un système probabiliste et économique par essence, donc c'est beaucoup plus fragile.

Comment cette faiblesse pourrait être exploitée ? Si vous pouviez reclasser les transactions jusqu'au moment où un nom a été enregistré, vous pourriez procéder à l'enregistrement de ce nom avant l'enregistrement légitime, et donc voler le nom.

Vous pourriez aussi faire en sorte que les opérations de renouvellement du nom aient lieu après la date d'expiration, ce qui ferait expirer le nom et vous permettrait de l'enregistrer vous-même. Aucun de ces scénarios ne s'est produit dans la vraie vie avec Namecoin. Mais si Namecoin attire un nombre croissant d'utilisateurs, davantage de gens pourraient être tentés de le faire.

Bitcoin a le même problème. Mais puisque Bitcoin est beaucoup plus utilisé que Namecoin, il est davantage protégé contre d'éventuelles attaques. Beaucoup de recherches sont menées pour résoudre ce problème de chaînes de blocs secondaires moins sûres que Bitcoin. C'est en partie dû au fait qu'un grand

nombre d'améliorations apportées à Bitcoin, y compris par des entreprises disposant de ressources élevées, sont bien plus faciles à mettre en œuvre si ce problème est réglé. Nous gardons donc un œil sur ces recherches et nous espérons que des progrès seront bientôt réalisés.

Aucune des solutions dont j'ai parlées concernant les programmes malveillants, les marques déposées et la vie privée ne sont aussi simples que les contre-mesures prises avec le DNS. Trouver des solutions plus « élégantes » dirons-nous est une question de recherche ouverte. Cela étant dit, dans beaucoup de situations réelles, ces solutions sont probablement suffisantes.

Bien. Qu'est-ce qui se passe en termes de développement ? Malheureusement, à l'heure actuelle, Namecoin est vraiment compliqué à installer, surtout si vous voulez faire fonctionner le protocole TLS. C'est principalement dû au fait qu'il n'est pas vraiment automatisé dans le processus d'installation. Nous venons de recevoir des fonds de la fondation NLNET et de l'Internet Hardening Fund sur le budget du ministère néerlandais des Affaires économiques. Ces fonds serviront à améliorer la facilité d'utilisation et le support d'application de Namecoin en tant qu'infrastructure de gestion de clés publiques TLS. Le but ultime ici, c'est d'intégrer Namecoin au système de résolution de nom d'un ordinateur. Avec les plus gros

navigateurs web, le protocole TLS pourra être installé en une seule étape. Par exemple, si vous utilisez Windows, vous lancez un programme d'installation .exe. Si vous utilisez Debian, vous lancez un programme .deb.

Ces fonds serviront aussi à apporter des améliorations UX pour les titulaires de noms, et pour faciliter la capacité d'évolution et obtenir une meilleure performance. Ce travail est principalement mené par moi-même, Hugo Landau, Brandon Roberts et Joseph Bisch.

Nous contribuons aussi activement au projet Tor. La base d'utilisateurs de Tor intègre des exigences de sécurité qui ne sont pas vraiment adaptées au DNS. Ils utilisent .ONION maintenant, qui génère des noms n'ayant pas de signification humaine, et les choses vont aller en empirant lorsqu'ils lanceront la version 3 de leurs services Onion, comme je l'ai montré plus tôt. Le problème, c'est que les humains ne vérifient généralement pas l'adresse entière .ONION, ce qui veut dire qu'au moment où je vous parle, des entités malveillantes créent des aperçus partiels d'adresses .ONION existantes pour se faire passer pour elles. Tor est un bon candidat pour adopter Namecoin. Ce système peut certainement s'accommoder des inconvénients de Namecoin, sauf peut-être pour la question du respect de la vie privée, parce que toutes les autres options

envisageables ne répondent tout simplement pas aux exigences de sécurité de Tor. C'est moi qui suis actuellement chargé de la collaboration avec le projet Tor.

La dernière partie du développement est bientôt terminée, nous aurons bientôt une hardfork. Pour ceux qui ne maîtrisent pas la terminologie des chaînes de blocs, il s'agit d'une mise à jour qui force complètement la rétrocompatibilité. C'est nécessaire parce que Bitcoin a fait des mises à jour de son système que l'on ne peut pas adopter sans forcer la rétrocompatibilité, et nous voulons rester proches du système Bitcoin.

Nous voulons aussi procéder à plusieurs autres mises à jour, notamment pour rendre la date d'expiration plus facile à gérer pour les utilisateurs, avoir des preuves de non-existence afin de démontrer facilement si un nom n'existe pas, ce qui permet aux nœuds de réseau d'archiver des données anciennes pour assurer une meilleure capacité d'évolution Les contenus hachés seraient conservés donc les données archivées pourraient toujours être prouvées, ce qui permettrait d'acheter des namecoins en utilisant des bitcoins, ou en passant par Monero ou Zcash, sans risque de contrepartie. Ces efforts sont en grande partie réalisés sous la direction de Daniel Kraft.

Merci de m'avoir invité. Je serais heureux de répondre à vos questions.

DAVID CONRAD : Bien. Merci Jeremy. Nous avons quelques minutes pour prendre des questions, si quelqu'un en a. Oui Steve ?

STEVE CROCKER : Excellente présentation. Merci beaucoup.

JEREMY RAND : Merci.

STEVE CROCKER : J'écoutais ce qui concerne le degré de protection et les situations où les choses peuvent déraper. Si je comprends bien, une protection forte permettrait d'avoir connaissance de toutes les modifications effectuées. Donc si l'on prend l'exemple de la zone racine, si l'on adoptait ce système, on saurait si quelqu'un modifie la zone racine. C'est un certain degré de protection mais l'une des questions qui intéressent certaines parties est : Comment je peux empêcher qu'une action nuisible à mon TLD soit réalisée ? Peut-être que la solution réside dans le système M-de-N combiné au fait qu'une personne lambda, celle qui procéderait normalement à la modification, est censée avoir une clé valide. Les autres clés seraient utilisées pour annuler des actions ou quelque chose comme ça. Mais je ne suis pas

totalement sûr que ce soient les seules choses qui puissent arriver.

JEREMY RAND : Vous pouvez effectivement utiliser Namecoin dans le but d'empêcher complètement des attaques malveillantes. Certaines choses comme la méthode de signatures multiples, les signatures M-de-N, peuvent servir à ça. C'est aussi le cas pour la politique d'authentification à deux facteurs, dont je parlais plus tôt.

Je pense qu'il y a plusieurs solutions. On peut aussi faire en sorte que tout acte malveillant soit signalé publiquement et ne soit pas effacé de la mémoire. Mais oui, vous avez tout à fait raison, c'est important de pouvoir déjouer les attaques le plus en amont possible. Et oui, Namecoin peut y contribuer. Étant donné que le système Namecoin a été conçu à la base pour les utilisateurs finaux qui possèdent un nom de domaine ordinaire, c'est possible – si vous craignez que votre bureau d'enregistrement nuise d'une manière quelconque à votre nom, par exemple qu'il laisse quelqu'un d'autre le mettre à jour accidentellement – si vous le souhaitez, de devenir votre propre bureau d'enregistrement. Ainsi, vous n'aurez pas à dépendre de tiers, à moins que vous ne vouliez qu'ils offrent une protection supplémentaire, comme les signatures multiples.

STEVE CROCKER : On peut avoir besoin de l'intervention d'un tiers pour plusieurs choses, comme l'attribution du nom, la récupération des clés si elles ont été perdues, la prévention ou la réaction à un comportement malveillant, etc. J'ai du mal à concevoir une variation du système dont nous disposons qui ne permette pas ce genre de transactions et évidemment, dès que vous vous passez de cette sécurité, vous vous exposez au risque de subir le comportement nuisible d'un opérateur. Il faut donc trouver un compromis.

JEREMY RAND : C'est ça oui.

STEVE CROCKER : Oh, juste une dernière chose.

JEREMY RAND : Oui ?

STEVE CROCKER : Le genre d'opérateurs nuisibles que nous craignons s'en ficheraient complètement d'être découverts.

JEREMY RAND : Oui, je pense que c'est vrai. Il faut effectivement trouver un juste milieu entre d'un côté, avoir une intervention humaine en cas d'action malveillante, et de l'autre, croire, en tant qu'utilisateur légitime, qu'un humain ne pourra pas nuire à notre nom. C'est fondamental. Il n'y a pas de bonne manière d'obtenir les deux types de protection en même temps. C'est pour cette raison qu'il est peu probable que Namecoin remplace complètement le DNS dans les temps à venir. En fait, je pense qu'un très grand nombre d'utilisateurs préfèrent le DNS à Namecoin pour cette raison. Cela étant, je pense qu'il existe aussi une base significative d'utilisateurs qui sont prêts à s'accommoder des compromis que représente Namecoin, quitte à ce que quelqu'un leur vole leur clé privée. Mais oui, c'est vraiment une question de recherche ouverte, rendre la protection des clés privées si élevée que les risques soient presque nuls. C'est une question de recherche ouverte.

STEVE CROCKER : Je poursuis rapidement. D'après ce que je sais de la technologie d'aujourd'hui, voler une clé privée est négligeable. Par contre, le risque de perdre le contrôle est beaucoup plus élevé si votre clé privée est détruite ou perdue, ou quelque chose dans le genre. C'est plutôt dans ces cas-là qu'il faudrait une solution.

JEREMY RAND : Oui. Si vous n'avez pas peur qu'une entité malveillante vous vole votre clé et vous craignez plutôt que votre clé soit détruite par accident, alors oui, c'est possible d'avoir une clé de secours. C'est possible par exemple d'avoir une politique de signatures multiples, du genre 1 de N, avoir N solutions de secours, désolé, N-1 solutions de secours. N1 veut dire que vous pouvez utiliser la clé principale pour tout et vous pouvez avoir un historique pour que les clés de secours ne puissent être utilisées pour récupérer le nom que si la clé principale est détruite et que, admettons, six mois se soient écoulés. Ce qui ne dépasse pas la date d'expiration du nom mais si quelqu'un essaye de se servir d'une de vos clés de secours, ça ne marchera pas à moins d'avoir aussi perdu la clé principale. C'est donc un système relativement flexible. Mais oui, à un certain point, vous comptez sur le fait qu'un certain nombre de clés ne seront pas perdues.

DAVID CONRAD : Bien. Il nous reste encore quelques minutes pour prendre des questions. Asha.

ASHA HEMRAJANI : Merci David. Merci pour cette présentation. Je dois dire que je n'en ai pas vraiment compris les trois quarts, donc j'ai simplifié

dans ma tête mais je voulais savoir si j'ai bon. Donc pour empêcher les attaques et protéger votre nom de domaine d'un gouvernement ou d'un bureau d'enregistrement, le DNS est installé sur l'ordinateur, le répertoire téléphonique numérique est en quelque sorte dans l'ordinateur.

JEREMY RAND : Oui.

ASHA HEMRAJANI : Et Bitcoin vérifie que chaque ordinateur a le même répertoire téléphonique numérique ou le même DNS, c'est bien ça ?

JEREMY RAND : Oui, c'est ça. C'est un très bon résumé.

ASHA HEMRAJANI : OK, super ! J'aimerais revenir à ce que tu disais sur .BIT plus tôt dans les diapos. Ça fait référence à tous les sites web .BIT, c'est ça ?

JEREMY RAND : Oui. Namecoin utilise actuellement le TLD .BIT et par conséquent, si vous avez installé le logiciel Namecoin, il

intercepte toutes les demandes DNS pour tout ce qui finit par .BIT et il regarde les noms en .BIT sur Namecoin plutôt que dans le DNS.

ASHA HEMRAJANI : OK. J'ai une question. Tu as dit que .BIT n'était pas enregistré auprès de l'ICANN. Est-ce que c'est obligatoire pour que ça fonctionne ?

JEREMY RAND : Ce n'est pas obligatoire pour que ça fonctionne du point de vue technique. Ça fonctionne déjà, même si ce n'est pas enregistré auprès de l'ICANN. Le problème, c'est que dans l'hypothèse où l'ICANN attribuerait le TLD .BIT à quelqu'un d'autre à l'avenir, on ne saurait pas vraiment comment le système est censé fonctionner. Les personnes qui auraient installé le logiciel Namecoin, tel qu'il existe actuellement, accèderaient aux sites web Namecoin en utilisant cette fonction de recherche, mais les personnes qui ne l'auraient pas installé accèderaient à l'entité à laquelle l'ICANN aura délégué .BIT. Et les uns ne pourraient pas avoir accès à la même chose que les autres. On a donc un risque de collision dans l'espace de noms. C'est pour ça qu'on aimerait vraiment pouvoir s'enregistrer officiellement pour éviter tout

risque que quelqu'un essaye d'acheter .BIT à l'ICANN à l'avenir et engendre des problèmes.

ASHA HEMRAJANI : OK. Ça m'aide vraiment. Merci beaucoup.

JEREMY RAND : Merci.

DAVID CONRAD : OK. Kaveh.

KAVEH RANJBAR : Merci Jeremy pour cette présentation. J'ai une question rapide. À ma connaissance, vous n'avez pas abordé le sujet avec l'IETF, à part pour évoquer brièvement .BIT pour le registre de noms à usage spécial. Est-ce que c'est voulu ou est-ce que vous prévoyez d'en parler à l'IETF ?

JEREMY RAND : C'est une très bonne question. Lorsque Namecoin a été créé en 2011 – et à l'époque, je n'y travaillais pas encore – les fondateurs n'avaient pas idée de l'importance du registre de noms à usage spécial. En gros, ils se sont dit : « Bon, on espère que l'ICANN ne

délèguera pas .BIT à quelqu'un d'autre. » Évidemment, ce n'était pas une super décision mais ils ne savaient pas qu'une autre voie était possible.

Plus récemment, lorsque Tor, I2P et Ganu.net ont essayé d'enregistrer leurs TLD par le biais du registre de noms à usage spécial, on en a entendu parler et on s'est dit que ça serait pas mal pour nous aussi. Alors on a contacté les auteurs de ce mécanisme internet, qui nous ont ajoutés. Malheureusement, pour des raisons politiques que je n'évoquerai pas parce que je ne suis pas le mieux placé pour en parler, ce projet a été mis de côté pour une durée indéterminée. Un nouveau mécanisme internet a finalement été accepté et c'est devenu un RFC qui n'a ajouté que .ONION, c'est-à-dire Tor. Donc les trois autres – Ganu.net, I2P et Namecoin – attendent que la situation évolue. On s'est lancés là-dedans avec enthousiasme mais peut-être qu'on n'a pas été assez rigoureux. Mais lorsque nous avons découvert qu'il existait un système que nous devrions adopter, nous avons fait ce que nous avons pu.

KAVEH RANJBAR : Merci beaucoup.

JEREMY RAND : Merci.

DAVID CONRAD : Warren et Daniel – ou plutôt Warren et puis toi, et on fermera la file d'attente – pour la prochaine présentation. Warren ?

WARREN KUMARI : L'une des choses qui m'inquiète, c'est que pour posséder un domaine, il faut une clé publique – pardon, je voulais dire privée – et vous pouvez faire plein de trucs sympa avec le système M-de-N mais les utilisateurs ont franchement du mal à comprendre une bonne partie de tout ça.

JEREMY RAND : Oui, tu as raison.

WARREN KUMARI : Disons qu'avec Bitcoin, je peux avoir mon propre portefeuille et je peux suivre tout ce que je fais moi-même, mais c'est trop compliqué pour la plupart des gens, qui préfèrent donc avoir des portefeuilles publics en ligne, mais ces portefeuilles peuvent être volés. Est-ce qu'il y a un travail de mené pour simplifier considérablement tout ça pour les utilisateurs, pour qu'ils comprennent exactement ce qu'ils font avec ça et n'étalent pas leurs informations au grand jour ?

JEREMY RAND : Oui, on travaille sur la question. Le gros du travail est réalisé par le personnel de Bitcoin et pas par nous, parce qu'ils disposent de bien plus de ressources que nous. Tu devrais trouver le GreenAddress dans Bitcoin très intéressant. En gros, c'est un portefeuille Bitcoin qu'on peut soit installer comme une application mobile, soit comme une extension dans ton navigateur. Mais ça cache un système d'authentification à deux facteurs. Et à moins d'avoir vraiment besoin de récupérer ses clés, au cas où ce service planterait, on n'a pas vraiment besoin de s'occuper soi-même de la gestion des clés. Ça permet de rendre les choses plus faciles pour les utilisateurs. Donc oui, on aimerait bien voir des systèmes comme GreenAddress chez Namecoin.

DAVID CONRAD : OK. Daniel.

DANIEL DARDAILLER : J'ai quelques questions. Tout d'abord, tu as commencé en disant que l'approche non déterministe de l'actuel DNS était un problème, mais dans quelle mesure est-ce un problème puisqu'une fois qu'un nom est enregistré, il passe par le bureau d'enregistrement et le registre, et ça se passe forcément de

façon déterministe ? Il y a le résolveur de noms, le cache, ça fonctionne comme une transaction dans une base de données de protocole. Donc quelle partie du problème déterministe vous essayez de résoudre ? Est-ce que c'est l'enregistrement en lui-même ou la résolution ? C'est ma première question.

Lié à ça, on a la question de la performance. Je veux dire qu'aujourd'hui, le système est conçu pour être très performant parce qu'il y a des millions de résolutions par seconde, et le système utilise des chaînes de bloc ou un journal interne *append-only*, un livre IP. Généralement, il faut l'intégralité du DNS pour prouver quelque chose en utilisant les clés cryptographiques, alors comment ça marche ? Je veux dire, au vu des contraintes relatives à la performance et au journal *append-only*.

JEREMY RAND : Oui, bonnes questions. En ce qui concerne le problème du non déterminisme, l'exemple que je donne souvent en ce moment, c'est que lorsque le service de réduction d'URL bit.ly a été enregistré au départ, les gens qui l'utilisaient ne se disaient probablement pas qu'un jour, .LY serait contrôlé par l'État islamique. Ce risque est maintenant bien réel et si Daech finit par contrôler .LY, qu'est-ce qu'il se passera ?

Par ailleurs, les bureaux d'enregistrement de noms de domaine font parfois des erreurs. C'est bien plus rare qu'avant, mais aux débuts du DNS, ces entités ont été manipulées et poussées à transférer des noms de domaine à d'autres personnes sans réelle autorisation, en envoyant de faux fax par exemple, ce genre de choses.

Donc je ne pense que ce soit un risque élevé en règle générale, mais ce risque existe quand même donc je pense que ça vaut la peine de chercher quelque chose qui agisse de façon déterministe.

En ce qui concerne la capacité d'évolution, tu as tout à fait raison, les chaînes de blocs et les structures de données *append-only* évoluent en général bien moins vite que des systèmes comme le DNS, c'est vrai. Pour être franc, pour le moment, c'est difficile d'imaginer à quel point quelque chose comme Namecoin peut évoluer. On a d'ailleurs eu une discussion plutôt intéressante à ce sujet hier au moment des questions-réponses, alors que je participais à un comité. Mais oui, il peut prendre beaucoup plus d'ampleur que maintenant. Je pense qu'il pourrait gérer la plupart des utilisateurs des services .ONION de Tor sans trop de problèmes, ce qui serait une bonne chose. Est-ce qu'il pourrait remplacer le DNS aujourd'hui ? Non, pas du

tout. Est-ce qu'il pourrait remplacer le DNS dans un avenir lointain ? Difficile à dire. Peut-être, peut-être pas.

DAVID CONRAD : OK. Merci. Je crois qu'on est légèrement en retard. Le prochain intervenant est Paul Vixie de Farsight Security, qui va nous parler des zones de politique de réponse.

Paul, c'est à toi.

PAUL VIXIE : Merci David. Tant qu'on est sur la question de l'ajout de couches d'actions au DNS ou au système de nommage en général parce que ça ne fonctionne pas comme on voudrait, j'ai ma propre solution.

Ce que je voudrais souligner en revanche, c'est que plusieurs responsables de l'ICANN ont dit à plusieurs reprises : « Nous ne sommes pas la police de l'Internet. » À chaque fois où presque, c'était en réponse à quelqu'un qui aurait souhaité que cette manipulation soit plus facile à faire, parce qu'il y aura forcément un nom de domaine quelque part lié à des ressources quelque part qui portera préjudice à quelqu'un. À l'époque d'avant Internet, on partait du principe que tout appartenait à quelqu'un et que si une chose était utilisée pour vous nuire, vous

pouviez découvrir qui était derrière ça et faire arrêter la personne, intenter une action en justice ou au moins lui faire parvenir votre plainte et l'enjoindre de remédier à la situation.

Donc le côté où Internet est une sorte de, je sais pas, un service de dilution des responsabilités auquel vous demandez sans arrêt de faire cesser des choses qui vous nuisent, mais au final, personne n'y peut rien et tout le monde dit « Désolé, je ne sais pas qui pourrait s'occuper de ça mais ce n'est pas moi », c'est très frustrant pour les personnes lésées par ce qui peut se passer sur Internet.

Vous pouvez vous plaindre de la météo autant que vous voulez, ou sortir et faire ce que vous voulez.

Diapo suivante.

Tous ceux que je vois sur ma droite le savent déjà, mais ceux qui sont à ma gauche ont peut-être besoin d'un rappel, donc pour le bien de George Sadowsky, laissez-moi expliquer tout ça.

[Rires]

PAUL VIXIE : Il existe trois couches dans le flux de données du DNS.

Tout en bas, vous avez les résolveurs basiques. Ce sont vos smartphones, vos ordinateurs portables, toutes les machines virtuelles. Presque tout ce qui émet une requête DNS est un résolveur basique. Et un résolveur basique veut entrer en contact avec un résolveur récursif, ce qui n'est franchement pas un joli nom. Nous avons besoin d'un meilleur département marketing sur ce coup-là.

Ne cherchez pas à comprendre de quelle récursivité on parle, prenez-le comme un mot neutre. Ce truc est capable de répondre à vos questions, y compris pour dire qu'il n'y a pas de réponse, que ce n'est pas le bon nom, qu'il n'y a pas de données ou je ne sais quoi.

Il procède avec un cache, comme vous le voyez à gauche, qui sert de lieu de stockage. Il ne s'agit généralement pas d'un disque de stockage comme sur l'image là, mais dans tous les cas, il se rappelle des réponses les plus récentes, donc si beaucoup de personnes demandent la même chose, vous n'avez pas besoin d'aller chercher sur Internet encore et encore.

Maintenant, si quelqu'un vous demande quelque chose qui n'est pas dans votre cache, voici ce que vous devez faire. Vous devez aller au niveau supérieur, où l'ICANN vit vraiment. Le monde de l'ICANN, ce sont les serveurs d'autorité. Les serveurs de noms racine, les serveurs TLD, les serveurs TLD effectifs, les registres,

les bureaux d'enregistrement, les titulaires de nom de domaine, tout c'est, c'est l'espace d'autorité.

Et donc, c'est par les serveurs d'autorité, du point de vue du protocole, que les contenus entrent dans le DNS depuis l'extérieur. Une fois dans le DNS, vous pouvez aller chercher les contenus en utilisant le protocole DNS, mais avant de pouvoir être trouvés, ils doivent être importés d'une manière ou d'une autre. Le plus souvent, c'est à partir d'un fichier texte, d'une base de données ou d'un logiciel. C'est la mission des autorités d'importer les contenus DNS depuis l'extérieur.

Ce qui est inhabituel à propos de cette présentation à une réunion de l'ICANN, c'est que nous n'allons pas parler des serveurs d'autorité ou des politiques à invoquer pour créer tel nom ou déterminer qui doit gérer quoi. D'habitude, lorsque j'assistais plus souvent à ce genre de choses, on passait beaucoup de temps à parler des serveurs d'autorités et des politiques liées, et c'est certainement là-dedans que va tout l'argent, mais pour changer, nous allons parler de la couche du milieu.

La raison à ça, c'est que les personnes lésées par le biais d'Internet veulent vraiment pouvoir faire quelque chose, et il apparaît qu'on ne peut pas empêcher les gens qui veulent vous nuire d'enregistrer des noms de domaine et d'ajouter des

contenus relatifs à ces noms qui vous porteront préjudice. Ce serait une solution radicale. Si l'on imagine qu'on est d'un côté d'Internet et que ces personnes sont de l'autre côté, on aimerait avoir une solution radicale pour empêcher, par exemple, l'atteinte aux marques ou à la propriété intellectuelle en général, ou la mise en ligne de contenus pédophiles. Ce sont des choses que l'on juge nuisibles et qu'on aimerait pouvoir empêcher totalement, mais ce n'est pas possible, parce qu'une fois de plus, Internet fonctionne comme un service de dilution des responsabilités. Donc ce à quoi nous sommes parvenus, pas par choix mais par nécessité, c'est une solution plus douce. Puisque nous ne pouvons pas empêcher ces actions ou les annuler de façon suffisamment fiable, je fais en sorte que ma vision du DNS soit compatible avec la non-existence de ce qui me nuit.

Cette approche connaît un grand succès. Nous avons lancé ce projet en 2011. Nous avons revu le protocole trois fois donc nous en sommes maintenant à la version 4. En ce moment, nous cherchons à normaliser le protocole actuel, après quoi nous donnerions le contrôle du protocole à l'IETF mais jusqu'ici, l'IETF n'avait pas grand-chose à voir avec tout ça.

C'était vraiment un travail d'équipe dans notre coin, un peu comme un projet à code source ouvert du genre de Namecoin.

On a pioché des idées parmi vous, pas parce que vous étiez de l'IETF, mais parce qu'on a pensé que vous étiez intelligents et qu'on a aimé ce que vous avez dit.

Ce que nous faisons, c'est faire en sorte que les observations et les analyses de personnes extérieures soient utilisées pour mettre au point une politique, qui prévoit la réponse à apporter. Je vais parler du Z dans un instant mais laissez-moi juste dire que le cache n'est pas concerné par tout ça.

Vous pouvez imaginer une politique du genre : « Hey, il y a un nouveau réseau zombie avec un algorithme de génération de domaines [DGA] qui crée plein de noms. Un peu comme Conficker ou un truc dans le genre. Nous voulons faire en sorte qu'une personne cherchant l'un de ces noms n'obtienne pas de réponse, parce que la réponse pourrait expliquer à l'un de mes bots ou à un client infecté sur mon réseau comment accéder à une commande et un serveur de contrôle sur le réseau de quelqu'un d'autre, et il faut que j'intercepte ça à un moment donné. Je décide de l'intercepter au niveau du DNS. »

Et vous pourriez dire : « OK, donc ces noms calculables que le réseau zombie va utiliser aujourd'hui sont interdits. » Ça pourrait être ça votre politique.

Mais demain, ça ne sera plus valable. Demain aura de nouveaux noms. Ces réseaux zombies avec un DGA utilisent la date du jour, entre autres, pour calculer les noms à utiliser. On ne veut pas bloquer les noms indéfiniment. Ça augmenterait considérablement le risque de collision, et il y a déjà des collisions alors que ces noms...

Un réseau zombie avec un DGA comme Conficker génère des noms vraiment moches mais qui entrent en conflit avec des noms tout aussi moches mais non malveillants. Il faut donc les supprimer.

C'est pour ça qu'on ne met pas la politique dans le cache. On met la vérité dans le cache.

Le mécanisme de politique de réponse ne concerne que ce qu'un résolveur basique voit. Ça ne concerne pas ce qui est stocké ou ce que les autorités vont chercher.

Je vous ai dit que j'allais parler du Z. Le Z, c'est la zone, et ça reflète le fait que ces serveurs de noms récursifs sont déjà présents sur Internet. Il en existe 25 millions, dont la majorité n'a rien à faire là. Ce sont des petits modems câbles stupides qui ne devraient pas proposer le service qu'ils proposent. Et environ deux millions d'entre eux ont été créés intentionnellement. Il y a donc environ deux millions de serveurs de noms récursifs qui

nous intéressent. Et puis il y a le DNS ouvert et Google avec son 8.8.8.8. Il y a beaucoup de serveurs de noms récursifs qui nous intéressent. Et ils sont... comment dire ça ?

Nous voulons pouvoir contrôler la politique de ces serveurs en utilisant des données externes – et bon nombre de ces serveurs existent bien cachés dans des réseaux existants – en leur mettant un pare-feux de malade pour qu'ils ne puissent pas entrer en contact avec l'extérieur ou être trouvés par des personnes extérieures.

On considère que c'est une bonne mesure de sécurité de mettre un pare-feux à vos serveurs de noms récursifs pour qu'ils ne soient pas utilisés comme des amplificateurs de DDOS par des personnes extérieures au réseau.

Mais nous avons remarqué que beaucoup d'entre eux sont autorisés à entrer en contact avec le protocole DNS hors réseau. Nous nous sommes donc dit que si l'on pouvait glisser la politique sous forme d'une donnée DNS à aller chercher sur le port TCP 53, de la même manière que d'autres données DNS, ça pourrait marcher, et ces serveurs de noms récursifs pourraient adhérer à une source de politiques. C'est comme ça qu'on a commencé à essayer de passer la politique de réponse sous la forme d'une zone DNS.

C'est la zone DNS la plus moche que vous puissiez voir. Elle est bourrée de motifs que l'on est pas censé trouver dans la vraie vie, c'est totalement pas naturel et vraiment horrible à voir.

On pourrait être fier de voir à quel point c'est horrible, comme si l'horreur en soi était un projet artistique.

Le principe, c'est que quelqu'un, ici en haut à droite, se charge de l'observation et de l'analyse. La personne se dit « OK, un nouveau réseau zombie, un nouveau DGA, une nouvelle série de noms qui ne devraient pas être résolus aujourd'hui, ou peut-être que c'est un nouveau bloc d'adresses IP qui est utilisé par un spammeur, et peut-être que le spammeur a une station de radio pirate et qu'il propose de l'espace BGP qui ne lui appartient pas, et on veut vraiment s'assurer qu'aucune réponse qui entraîne un enregistrement A ou AAAA et qui se trouve dans cet espace piraté ne soit résolue aujourd'hui. »

Donc vous balancez toutes ces conclusions de l'observation et de l'analyse dans la zone de politique de réponse, dans laquelle les serveurs de noms récursifs entrent par le biais de la méthode de transfert de zone normale.

Je tiens à préciser qu'il s'agit d'une action intentionnelle. L'opérateur du serveur de noms récursif doit vouloir faire ça. Il

ne s'agit pas du SOPA. Il ne s'agit pas de quelque chose que quelqu'un vous fait en amont et que vous ne pouvez pas éviter.

Par ailleurs, si votre serveur de noms récursif adhère à l'une de ces choses et que vous la détestez, vous pouvez passer au 8.8.8.8, donc tout ça reste très intentionnel, même pour un résolveur basique. Cette méthode, même si elle peut être utilisée pour essayer de mener un travail de censure, n'existe pas. Elle doit être vue comme une valeur ajoutée ou elle ne sera jamais utilisée par l'opérateur du serveur de noms récursif ou par celui du résolveur basique.

Je voulais le préciser.

Donc, que sont ces chiffres ? Un serveur de noms récursif peut faire tourner BIND ou Unbound en utilisant un logiciel quelconque, ou PowerDNS ou... il y en a un quatrième. Il existe quatre services d'exécution indépendants qui ne partagent aucun code source mais qui interagissent très bien entre eux. Dans le monde de l'IETF, si vous avez plusieurs exécutions interopérables, alors vous commencez à penser que le document de protocole est complet. Avec quatre services, je pense que ça couvre à peu près tout.

Il existe des milliers de serveurs de noms récursifs qui adhèrent à une ou plusieurs zones de politique de réponse [RPZ]. Et il existe

une dizaine de services de sécurité qui publient leurs observations et analyses sur ce forum. Rod Rasmussen en représentait un jusqu'à récemment.

Il y a un site web, dnsrpz.info, qui contient la liste de toutes ces exécutions, de tous les contributeurs, et qui renvoie vers la spécification. C'est ce que la communauté fait pour se protéger de son côté des problèmes qui surviennent de l'autre côté, là où l'on ne peut pas les empêcher. Et ça marche. Ça marche vraiment très bien.

Mon entreprise propose maintenant une politique de sécurité dans ce format de zone, qui a été très bien reçue. Et il me semble que Rod a eu des bons résultats avec dans sa dernière entreprise. C'est donc bien pour le secteur de la sécurité parce que ça nous permet d'avoir plus de clients. C'est aussi une bonne chose pour les personnes qui essayent de se défendre, parce que ça leur permet d'avoir un goulet d'étranglement dans leur réseau. Une solution très flexible consiste à avoir un service de vendeurs multiples associé aux politiques de sécurité auxquelles les gens veulent adhérer.

Dernière chose, mais non des moindres, il existe une solution d'entreprise. Rod et moi-même travaillons dans le secteur de la vente de ces politiques, mais c'est aussi très courant pour les banques, par exemple, d'avoir une liste de choses qu'elles ne

veulent pas résoudre aujourd'hui. Sans cette technologie, elles créent des zones vides n'importe où dans l'espace de noms qu'elles veulent pour, en gros, mettre du Tipp-Ex pour cacher certaines choses. Donc si vous en avez six millions et que vous en cachez la moitié chaque jour, ça donne un taux de déperdition énorme dans la configuration de votre serveur de noms. Alors qu'avec quelque chose comme la RPZ, vous ne changez pas la configuration de votre serveur de noms. Vous modifiez juste la politique de réponse. C'est une opération très simple.

Inévitablement, les personnes qui installent cet outil commencent par créer une RPZ qui est gérée par leur propre département de sécurité, qui, lorsqu'il se rend compte qu'il y a une menace – une fois encore, c'est une observation et une analyse – peut en quelque sorte balancer la politique de réponse dans le serveur de noms récursif, un peu comme dans une matrice où vous balancez quelque chose quelque part et ça se synchronise dans l'ensemble de la matrice. L'entreprise ne répond donc plus à certaines questions, ou ne répond plus à des questions qui entraîneraient certaines réponses en particulier.

On pourrait avoir d'autres politiques du genre : « On ne répond rien si on a affaire à un nom en particulier d'un serveur de noms. » Vous pouvez donc infecter des contenus sans connaître

la question ou la réponse, mais si vous savez que ça vient d'un nom ou d'une adresse IP d'un serveur de noms en particulier, c'est une mauvaise nouvelle. Ce n'est pas ça qui manque. Comme me l'a dit David Conrad une fois, on a assez de corde pour ceux qui voudraient se pendre.

Je pense que la dernière chose à dire, c'est qu'en général, on se dit « Je préfère mentir » et faire comme si quelque chose n'existait pas. En d'autres mots, c'est un faux signal NXDOMAIN. NXDOMAIN est la valeur de code retour dans le DNS qui indique que votre question fait référence à quelque chose qui n'existe pas. Mais c'est loin d'être la seule chose que vous puissiez faire, parce que beaucoup de gens ne veulent pas faire ça. Ces personnes peuvent créer ce qu'on appelle un jardin clos où... disons que vous cherchez un nom Conficker, un réseau zombie Conficker avec un DGA. Peut-être que vous voulez vraiment avoir un message *pop-up* qui s'affiche sur votre écran pour dire : « Hey, tu es infecté par Conficker. » Vous pouvez effectivement faire ça. Au lieu de répondre avec un faux NXDOMAIN, vous répondez avec un faux pseudo pour dire que le nom autorisé de ce que vous cherchez est jardinclos.exemple.com. Le serveur web d'une entreprise peut alors dire aux gens : « Hey, vous êtes probablement infectés, vous devriez appeler le département

informatique maintenant. » Il y a plein d'autres choses à faire à part mentir sur l'existence de quelque chose.

Je pense que c'est vraiment la dernière chose à dire avant de passer aux questions-réponses, nous mentons. Tout ça, ce sont des mensonges. L'autorité appartient à quelqu'un que vous pensez être malveillant et vous ne voulez pas connaître la vérité. Alors vous décidez de vous mentir à vous-même parce que c'est le moyen d'amener votre réseau et vos ressources à réagir à une menace en particulier. Lorsque vous mentez, ça interrompt le fonctionnement des DNSSEC, entre autres. Les DNSSEC ont une importance cruciale pour l'avenir de l'économie mondiale. Elles sont absolument nécessaires, pas seulement pour la DANE mais aussi pour toutes les autres applications qui les reconnaissent et qui en sont à diverses étapes de développement. Et ça interrompt leur fonctionnement. Si vous lancez ça et que les données elles-mêmes sont signées par l'autorité, notre code l'ignorera. Notre code n'applique pas de politique aux noms ayant une signature DNSSEC. Et les méchants ont un moyen très facile de contourner ça, il suffit de lancer les DNSSEC.

En revanche, le résolveur basique doit aussi faire une requête de DNSSEC. Il n'y a pas assez de DNSSEC partout pour empêcher ça. Mais à un moment donné, ça va poser problème. Je suis certain que lorsque la spécification actuelle sera publiée et que l'IETF

prendra le contrôle, il y aura presque immédiatement un nouveau protocole très similaire à celui-ci, sauf qu'il traitera les DNSSEC d'une façon un peu plus sensée. C'est une faille, nous le savons, mais pour le moment, ça ne nous affecte pas. Mais je souhaite vraiment que ce soit le cas parce que les DNSSEC deviendront alors omniprésentes et c'est ce dont nous avons besoin. C'est tout en ce qui concerne ce que j'avais préparé, je suis prêt à répondre aux questions. David, il nous reste combien de minutes ?

DAVID CONRAD : Nous avons cinq ou sept minutes pour prendre des questions pour Paul. Qui veut commencer ?

Personne n'a de questions pour Paul ? OK. Je vais commencer.

[Rires]

Paul, j'imagine que la RPZ exacerbe en quelque sorte les problèmes que beaucoup de nouveaux gTLD ont avec l'acceptation universelle. Premièrement, est-ce que c'est bien ça ? Deuxièmement, est-ce qu'il existe un moyen de gérer ça ?

PAUL VIXIE : J'ai un fils qui a travaillé pendant un temps dans le secteur des noms de domaine. Et quand .ENTERPRISES est devenu

disponible, il a enregistré le nom VIXIE.ENTERPRISES, ce que j'ai trouvé vraiment mignon vu que j'avais un cabinet de conseil avant sa naissance.

Il a ensuite essayé de l'utiliser et a découvert que United Airlines ne s'attendait pas à ce que vous associez .ENTERPRISES à votre compte. Heureusement, je connaissais quelqu'un chez United et j'ai pu régler ça. Mais il a eu beaucoup d'autres ennuis. Je comprends parfaitement que ces nouveaux gTLD soient compliqués à utiliser parce que beaucoup de personnes pensent que ça se limite à .COM, .NET, .ORG, .INFO ou à des ccTLD, et que si ce n'est pas ça, ça doit être une erreur. Je comprends. Mais ça ne vient pas de la RPZ et je n'ai jamais entendu parler de soucis liés à la RPZ.

DAVID CONRAD : OK. Tu as dit que la RPZ ne fonctionnait pas avec les DNSSEC. Je pensais que la RPZ fonctionnait avec les DNSSEC dans le sens où si une zone comportait une signature, la réponse revenait pour être validée et pouvait être validée. Et une fois validée, la réponse renvoyée au résolveur basique était modifiée comme indiqué par la RPZ.

PAUL VIXIE : C'est presque ça. Ça va certainement marcher de cette manière si le résolveur ne lance pas de requête de DNSSEC. Si on n'établit pas que D.O. = 1, alors il se passe ce que tu as dit. On va chercher les données. On les valide si possible. On les met dans le cache. Et ensuite, quand on essaye de formuler une réponse à la question originelle, on se dit : « Hey, mais il y a une politique. » Et puisque le résolveur n'a pas lancé de requête de DNSSEC, on va inventer quelque chose parce que si le résolveur ne peut pas détecter si l'on ment, alors on ment. Mais si le résolveur demande des enregistrements du DNS et qu'il y en a, alors on n'applique pas la politique.

DAVID CONRAD : George ?

GEORGE SADOWSKY : Merci Paul pour le rappel. Je suis presque prêt à faire le test.

J'ai une question qui concerne plus les personnes qui produisent les informations sur lesquelles repose la politique.

Je parle de la durée de vie. À quelle fréquence il faut les diffuser ? À quelle fréquence est-ce que vous faites les modifications à donner aux utilisateurs? Comment vous pouvez connaître leur durée de vie ?

PAUL VIXIE : Crois-le ou non, je suis content que tu poses cette question. La connexion est directe. Donc si l'on fait une modification, puisque nous sommes dans une zone DNS normale, ça envoie une notification, on a un transfert de zone différentiel, et la mise à jour se fait de façon quasi instantanée. Admettons que vous changiez d'avis au bout de 10 minutes et que vous modifiez la politique, ça se verra immédiatement dans l'ensemble de votre base d'utilisateurs. C'est très important pour nous de ne pas lancer quelque chose de totalement nouveau. Nous ne voulions pas de données obsolètes dans le système. Je vais vous donner un exemple.

Mon entreprise vend un nouveau service de domaine. Nous avons remarqué qu'il y avait 2,5 nouveaux points de délégation créés sur Internet chaque seconde, et la moitié d'entre eux disparaît probablement dans les 24 heures. Un sixième d'entre eux disparaît au bout de 10 minutes. C'est un taux de déperdition très élevé. Ces choses sont créées dans le but d'embêter quelqu'un et sont supprimées presque aussitôt la plupart du temps, ou mises dans une liste noire par des entités comme SpamHaus. Ça ne veut pas dire que tout ce qui est nouveau est mauvais, mais statistiquement, il y a de grandes chances que ce soit le cas.

Puisque je me rappelle de la joyeuse époque où lorsqu'on demandait un nom .COM après mardi, on ne l'avait que le vendredi, je m'accommode du fait que les nouveaux noms de domaine ne fonctionnent pas si bien que ça. Tout ce que l'ICANN et son écosystème ont mis en place pour réduire ce temps à 30 secondes n'a pas vraiment d'utilisation non malveillante dont je puisse me soucier.

Ça veut dire qu'il faut envoyer une mise à jour par seconde aux utilisateurs de notre RPZ pour leur dire : « Voici les nouveaux noms de domaine observés. Au fait, nous supprimons ceux qui existent depuis plus de 10 minutes parce que vous ne voulez que les nouveaux et ceux qui sont là depuis plus de 10 minutes ne sont pas nouveaux, selon votre définition. » Nous avons des définitions différentes.

Les réseaux, en envoyant des mises à jour toutes les secondes, peuvent synchroniser la politique de réponse auprès de milliers de faux clients ou de dizaines de vrais clients. Et ça marche. Ça se fait de façon très fluide. Il n'y a aucune donnée obsolète.

DAVID CONRAD : Warren ?

WARREN KUMARI : J'ai plus une remarque qu'une question. Avant, je gérais mon propre serveur de noms pour quelques domaines, mais je recevais tellement de courriers indésirables que j'ai fini par tout couper.

Et puis je me suis abonné aux flux RPZ de plusieurs personnes, et j'ai tout relancé, parce qu'avec la RPZ, je ne reçois presque pas de courriers indésirables. Je reçois des trucs de personnes qui ont une RPZ. Ça se gère tout seul et ça remarche très bien.

PAUL VIXIE : Merci pour cette remarque. J'aimerais y répondre.

Ce n'est pas possible de réaliser quoi que ce soit sur Internet si le DNS ne fonctionne pas. Je sais qu'il existe plein de protocoles *peer-to-peer* et donc tous les utilisateurs de BitTorrent savent quand le DNS ne fonctionne pas. Mais pour le reste d'entre nous, lorsque le DNS ne fonctionne pas, on se fiche de savoir ce qui est accessible puisqu'on ne va pas taper des adresses IP. On ne va certainement pas taper des adresses IPv6.

Maintenant, ça marche aussi pour les méchants. Il n'y a pas que les gentils qui ne peuvent rien faire si le DNS ne marche pas. Les méchants sont inaccessibles s'ils ne sont pas dans le DNS.

Tu as parlé de courriers indésirables. Pour moi, ce n'est plus un problème.

J'ai mon serveur de messagerie, Postfix, qui est configuré de façon à vérifier dans le DNS tous les noms qui apparaissent, que ce soit dans l'objet ou dans le message. Et s'il ne trouve pas un nom, je jette le message, ce qui veut dire qu'utiliser ce goulet d'étranglement comme endroit pour dire que tel ou tel nom ne devrait pas exister, s'ils existent, et mentir en disant qu'ils n'existent pas, peut provoquer toutes sortes de problèmes dans votre infrastructure. Il faut être préparé. Ça peut être surprenant si vous ne recevez pas ces courriers indésirables. En fait, ce dont tu as parlé est un but secondaire de tout ça.

DAVID CONRAD : OK. Merci Paul pour ta présentation sur la RPZ. On passe à Paul Wouters.

PAUL WOUTERS : Merci.

Puisque j'ai le micro, j'aimerais faire une petite remarque. Je dois dire que Paul Vixie et John Gilmore sont les deux personnes les plus difficiles à contacter par mail au monde, à cause de tous

leurs systèmes de protection en place ou de l'absence de systèmes de protection.

Cela étant...

>> (hors micro)

PAUL WOUTERS : Je suis un joyeux dommage collatéral.

Ça a été difficile de déployer les DNSSEC à large échelle. L'enregistrement DS que les gens ont besoin d'entrer dans leur zone mère est un processus très compliqué et qui implique beaucoup trop d'humains. La personne la plus importante là-dedans travaille pour le titulaire de nom de domaine et ne sait pas vraiment comment ça fonctionne. Il a juste acheté un service et un nom de domaine et il n'y connaît rien. Il veut juste que ça fonctionne. Il a un opérateur de domaine qui gère tout pour lui. Ils ne savent même pas ce que sont les DNSSEC et comment les activer, et même si l'opérateur du DNS leur dit quoi faire, ils ont un mal fou à y arriver.

Il existe beaucoup de domaines [inaudible] de gros services d'hébergement qui sont signés mais pas délégués avec un enregistrement DS, donc même s'ils sont fiables en eux-mêmes,

ils sont un peu tous seuls dans leur coin parce que l'enregistrement DS n'a pas été entré dans la zone mère, parce que c'est impossible à faire.

Et il fallait apporter une solution au problème.

Au début l'IETF n'a pas voulu s'attaquer à ça, mais à un moment donné, le problème est devenu trop important, alors l'IETF s'y est remis... et ça devient confus. Je vais fermer mon ordinateur.

Les deux choses dont ils avaient besoin – et ça existe maintenant avec le RFC-8078 publié la semaine dernière – c'était de trouver un moyen quelconque pour que l'opérateur du DNS signale au registre que tel domaine contient maintenant un enregistrement DS et lui demande de publier cet enregistrement.

L'autre chose, c'est que les opérateurs du DNS ont aussi besoin d'un moyen de dire « mon client s'en va » ou « mon client ne veut plus des DNSSEC ». Nous avons besoin d'un moyen de dire au registre de supprimer cet enregistrement lorsque les DNSSEC ne sont plus requises.

Et ce RFC permet cela. Il permet d'utiliser l'enregistrement de type CDS, qui est en gros le même que l'enregistrement DS, mais publié du côté du client, dans la zone client.

Et une fois que c'est publié, vous pouvez contacter votre registre et lui dire : « Hey, j'ai publié cet enregistrement CDS. Est-ce que vous pouvez jeter un œil et si c'est bon, le publier comme enregistrement DS dans votre zone mère ? »

Et c'est ce que le nouvel enregistrement fait.

Pardon. Ce n'est pas l'enregistrement qui fait ça. Cette façon de faire est toute nouvelle.

Il y a plusieurs moyens de contacter votre registre, ça dépend d'autres mécanismes. Il y a actuellement un autre projet en cours d'élaboration, qui consiste à utiliser une interface RESTful via le HTTP pour diffuser cette information, mais les gens peuvent proposer d'autres mécanismes à cette fin. Alors on a l'enregistrement spécial à annuler, c'est-à-dire l'enregistrement CDS avec tous les zéros, et on demande : « Merci de bien vouloir annuler ça, on ne veut rien. »

Il y a une coquille sur la diapo. Il devrait y avoir un quatrième zéro. On a repéré cette erreur lors de la dernière révision du mécanisme. Nous avons corrigé ça à temps pour la publication du RFC mais comme vous pouvez le voir, je n'ai pas modifié ma diapo.

Donc ce système fonctionne. Il y a aussi de nouvelles extensions EPP. Une fois que le registre a accepté cette sorte de mise à jour

externe de l'opérateur du DNS, il peut indiquer à son bureau d'enregistrement que cet enregistrement a été mis à jour et n'est pas passé par un flux EPP habituel.

Ce système est en cours de déploiement pour un certain nombre de TLD. Ça veut dire que bientôt, des centaines de milliers de nouveaux domaines ayant une signature DNSSEC seront délégués, et ça devrait faire considérablement avancer le déploiement des DNSSEC. On espère que ce sera un franc succès.

DAVID CONRAD : OK. D'autres questions pour Paul ?

Oui Lars ?

LARS JOHAN-LIMAN : Lars Liman. Je voudrais juste avoir une précision. On parle bien de l'enregistrement CDS proposé par, je crois que c'était par Olaf Kolkman ? Ou est-ce qu'on parle de celui qui tournait au sein de l'IETF ?

PAUL WOUTERS : Oui. Il s'agit bien du RFC d'Olaf Kolkman.

LARS JOHAN-LIMAN : Très bien. Merci. Ça met un peu l'accent sur l'absence de relation formelle entre les opérateurs du DNS et les registres, je pense que c'est une bonne chose.

PAUL WOUTERS : Je n'ai pas utilisé ce mot intentionnellement.

DAVID CONRAD : Patrik ?

PATRIK FÄLTSTRÖM : Est-ce que tu regardais

vers ta gauche ?

[Rires]

PATRIK FÄLTSTRÖM : Donc ce qui se passe en temps normal... si l'on peut revenir à la diapo, s'il vous plait.

En temps normal, la transaction DNSSEC passe par le bureau d'enregistrement, donc celui-ci a l'entière responsabilité de s'assurer qu'il a tous les éléments relatifs au titulaire de nom de domaine, y compris en ce qui concerne la clé.

Dans ce cas, la mise à jour de la clé se fait entre l'opérateur du DNS et le registre, sans passer par le bureau d'enregistrement, c'est bien ça ?

PAUL WOUTERS : C'est ça.

PATRIK FÄLTSTRÖM : Et tu dis que ce processus est déclenché par un événement dans l'EPP, c'est ça ?

Donc le bureau d'enregistrement est censé activer la commande pour aller chercher les informations concernant la nouvelle clé.

C'est ça le but ?

Ce que je crains, c'est que le bureau d'enregistrement n'ait soudainement plus de vision globale de la zone, ce qui peut avoir un impact sur les responsabilités du bureau d'enregistrement par rapport au registre.

PAUL WOUTERS : C'est tout à fait ça. Mais je crois comprendre qu'il y a une nouvelle extension EPP qui permet au registre d'envoyer les infos, donc le bureau d'enregistrement n'a pas besoin d'aller les chercher.

PATRIK FÄLTSTRÖM : Absolument. Il y a des extensions qui permettent de faire ça. Mais l'EPP est conçu pour que les bureaux d'enregistrement puissent mettre à jour le registre, et non l'inverse.

PAUL WOUTERS : C'est ça.

PATRIK FÄLTSTRÖM : OK. Il y a encore autre chose, lorsque le registre ordonne une modification dans l'automate du bureau d'enregistrement. Ça n'arrive que rarement, non ?

PAUL WOUTERS : C'est ça. Mais le bureau d'enregistrement peut aussi soutenir le même mécanisme et entrer en contact avec le titulaire de nom de domaine.

Ceux qui sont prêts à appliquer tous les paramètres des DNSSEC sans avoir à contourner le problème n'ont pas besoin de l'automate. Du moment que le bureau d'enregistrement et l'opérateur du DNS entretiennent une bonne relation de travail et peuvent se parler. Parce que si le bureau d'enregistrement ne peut pas parler avec l'opérateur du DNS, alors le problème

subsiste. Impossible de faire passer l'information sans utiliser ce mécanisme.

PATRIK FÄLTSTRÖM : [inaudible] comme en lançant une requête DNS, c'est ça ?

En tout cas, dans un but de transparence, lorsque j'ai lu ce document, j'ai suggéré qu'il normalise cet excellent enregistrement CDS, que ce soit le registre ou le bureau d'enregistrement qui aille le chercher.

PAUL WOUTERS : Où est-ce que le bureau d'enregistrement pourrait le publier ? Tu veux dire si le bureau d'enregistrement l'envoie via l'EPP ?

PATRIK FÄLTSTRÖM : Non, je veux dire que le bureau d'enregistrement va chercher le nouveau DS auprès de l'opérateur du DNS et l'envoie au registre via l'EPP.

PAUL WOUTERS : C'est déjà possible sans ce mécanisme.

DAVID CONRAD : Donc...

PATRIK FÄLTSTRÖM : Clôturons le sujet. Je l'ai déjà expliqué à la liste de diffusion de l'IETF, je n'ai sans doute pas besoin de recommencer.

DAVID CONRAD : Oui. Dan et puis Warren.

DAN YORK : Je voulais juste remercier Paul pour sa présentation. Je pense que le but, à mon avis, pour les membres du Conseil d'administration et les autres personnes qui nous écoutent sans vouloir entrer dans les détails, est simplement de comprendre que tout cela s'inscrit dans le cadre d'un travail plus global qui vise à proposer une meilleure automatisation dans le fonctionnement des DNSSEC. Au moment du déploiement à grande échelle des DNSSEC par les opérateurs du DNS ou d'autres personnes qui s'y sont essayées, l'une des principales difficultés était de transmettre ces informations, les enregistrements DS, aux registres.

C'est donc l'un des mécanismes dont disposent les registres, qui choisissent de s'en servir pour contribuer à l'automatisation de la publication d'informations et améliorer les choses, ce qui engendrera finalement un DNS plus sûr.

Ce qu'il faut retenir, c'est qu'on a un nouveau mécanisme disponible et les registres peuvent le voir comme un moyen de faire marcher tout ça.

Et pour revenir à ce que disait Patrik, les bureaux d'enregistrement pourraient aussi se pencher sur la question.

DAVID CONRAD : Warren ?

WARREN KUMARI : La raison pour laquelle j'ai essayé d'interrompre Patrik, c'est que je pense que tout le monde ne parlait pas de la même chose.

Lars, tu as dit qu'à l'origine, Olaf – en fait c'est Olafur – et moi-même étions derrière ce projet.

Le document original ne donnait pas la possibilité aux gens de cesser la publication automatique de ces enregistrements. Il fallait passer par le registre ou le bureau d'enregistrement, je pense que c'est ce dont Patrik parlait. Nous avons volontairement laissé de côté la partie « vous pouvez contourner votre bureau d'enregistrement » pour les mêmes raisons évoquées par Patrik. Ce projet repose sur d'anciens documents

et comprend de nouvelles caractéristiques. Mais peut-être que j'ai mal compris.

PATRIK FÄLTSTRÖM : Ce que j'essaye de faire, c'est séparer la fonctionnalité technique – c'est-à-dire la capacité d'un opérateur du DNS à signaler qu'il y a de nouvelles informations concernant une clé – du potentiel impact en termes de politique en ce qui concerne la relation entre le titulaire de nom de domaine, le bureau d'enregistrement et le registre. Cette discussion est totalement différente et pourrait poser problème pour certains TLD.

DAVID CONRAD : Je peux répondre rapidement ?

>> Patrik, le problème fondamental qui doit être réglé, c'est déterminer qui est le titulaire de nom de domaine et par quel moyen communiquer avec lui. Nous avons un nombre limité de registres donc on peut commencer par les contacter, mais ce serait bien si d'une manière ou d'une autre, on pouvait entrer dans le RDAP ou un autre protocole, trouver les coordonnées de l'entité prête à discuter avec nous, de préférence le registre ou

un revendeur, ou même le revendeur d'un revendeur. Mais c'est précisément ce que personne n'arrive pas à obtenir aujourd'hui.

DAVID CONRAD : Dmitry ?

DMITRY KOHMANYUK : Bonjour. Je voulais juste faire un commentaire rapide. Pourquoi la case registre est en double ? J'imagine que c'est une erreur ? Ensuite, j'aimerais appuyer les propos de Patrik Fältström par rapport au modèle EPP. Au fait, je représente l'un des TLD EPP en Ukraine. Je pense que ce modèle ne convient pas [inaudible]. Je pense aussi que le modèle de recherche est mal conçu et ne peut pas évoluer. L'EPP supporte les mises à jour DS mais mon plus grand souci ici, c'est qu'on essaye de séparer les enregistrements NS et la gestion des enregistrement DS. Ce n'est pas une bonne chose. Parce que changer d'opérateur du DNS peut entraîner des modifications des enregistrements DS et des enregistrements du DNS. Ça semble un peu bizarre que les mises à jour DS soient censées [inaudible] ce mécanisme sans supervision de l'enregistrement du DNS.

Je pense qu'on devrait revenir en arrière et examiner cette séparation entre les mises à jour de données – les noms, les adresses, etc. – et les données techniques dans un bureau

d'enregistrement. Je pense que c'est une bonne idée de laisser tomber l'opérateur technique tiers, mais c'est la mauvais solution. On n'a alors plus de relation contractuelle entre l'opérateur du DNS et le registre et ce n'est pas une bonne chose, ce n'est pas la façon de régler la situation et ça ne rendra pas Internet plus sûr.

Donc bien essayé mais...

PAUL WOUTERS : Juste très rapidement, et je passerai ensuite la parole à Paul Vixie.

Il y a eu une longue discussion à l'IETF à propos des déclencheurs et des temporisateurs, on va tâcher de ne pas recommencer.

C'est une option que les registres peuvent choisir, donc si certains registres ne peuvent pas le faire pour des raisons contractuelles ou ne veulent pas le faire, pas de souci, mais cette option sera utile à un grand nombre de personnes qui ne peuvent actuellement pas mettre les enregistrements DS là où ils devraient aller.

DMITRY KOHMANYUK : Oui. Il y a beaucoup de problèmes. Je ne crois pas qu'on doive discuter de ça ici. Mieux vaut en parler au sein de l'IETF. Merci.

PAUL WOUTERS : OK.

DAVID CONRAD : Paul ?

PAUL VIXIE : J'allais revenir sur ce point. Le NomCom travaille très dur pour que les personnes les plus qualifiées veuillent bien participer à ce conseil, et ces personnes ne sont pas forcément aussi calées en questions techniques que celles qui utilisaient Internet avant la création de l'ICANN. Nous devons utiliser leur temps à bon escient et respecter leur temps, donc si vous pouviez placer vos arguments à un niveau que George Sadowsky puisse comprendre...

[Rires]

DAVID CONRAD : Et sur ce, passons à autre chose.

Vous savez, on a essayé de restructurer en quelque sorte le fonctionnement du TEG. Nous avons fourni des rapports d'une ou deux pages aux membres du Conseil d'administration avant cette réunion et je me demande si ça a servi à quelque chose ou si nous devrions continuer de faire évoluer le TEG de façon à le rendre plus utile aux membres du Conseil.

Vous pouvez dire ce que vous en pensez maintenant ou m'envoyer un courriel, ou me traquer au cocktail qui va suivre. Les navettes partent dans environ 15 minutes. Sur ce, je clos cette session du TEG et je vous remercie pour votre participation.

[Applaudissements]

[FIN DE LA TRANSCRIPTION]